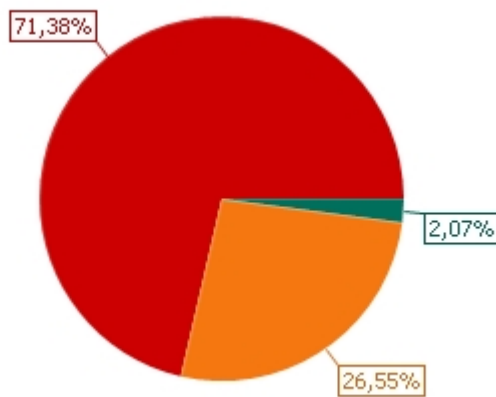


№ отчёта	fe48302c-9905-4ee5-89b3-62d537dc1ef3
Профиль	Уязвимости
Задание	Job_5302
Начало/завершение сканирования	19.05.2015 10:53:13 / 19.05.2015 10:54:53
Формирование отчёта	19.05.2015 15:30:20
Имя	Quick_localhost_191
Описание	Автогенерируемый отчет вкладки "История" для "localhost" из "Job_5302" задания.
Хосты [1]	localhost

### Диаграмма распределения уязвимостей по уровням риска



Риск	Количество
<b>Высокий</b>	207
<b>Средний</b>	77
<b>Низкий</b>	6
<b>Всего</b>	290

### Таблица распределения уязвимостей по хостам

Хост / Риск	Высокий	Средний	Низкий	Всего
localhost	207	77	6	290
<b>Всего</b>	<b>207</b>	<b>77</b>	<b>6</b>	<b>290</b>

### Таблица распределения уязвимостей по продуктам

Продукт / Риск	Высокий	Средний	Низкий	Всего
сре:/a:oracle:database_server	11	37	6	54
сре:/a:adobe:shockwave_player	150	2	0	152
сре:/a:adobe:adobe_air	38	9	0	47
сре:/o:microsoft:windows_7::sp1:x64	2	1	0	3
сре:/a:adobe:flash_player	10	7	0	17

cpe:/a:adobe:shockwave_flash_active x	10	7	0	17
cpe:/a:oracle:jre:1.8.0	6	7	0	13
cpe:/a:microsoft:sql_server:2012	0	2	0	2
cpe:/a:wireshark:wireshark	0	16	0	16
cpe:/o:microsoft:windows	0	3	0	3
<b>Bcero</b>	<b>207</b>	<b>77</b>	<b>6</b>	<b>290</b>

## Хост: localhost

CPE	cpe:/o:microsoft:windows_7::enterprise			
Начало/завершение сканирования	19.05.2015 10:53:13 / 19.05.2015 10:54:53			
Профиль	Нет			
Агент	Нет			
Тип сканирования	Быстрое			
Уязвимостей найдено	290:	207	77	6

## Уязвимости [290]

Хост	ALTX ID	Риск	Название
localhost	23646	Высокий	Неопределённая уязвимость в Spatial компоненте Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2012-3220)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	23709	Высокий	Уязвимость в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1292)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23710	Высокий	Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1291)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	64344	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0576)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	64345	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0577)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	23719	Высокий	Уязвимость в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1281)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23218	Высокий	Переполнение кучи в TextXtra.x32 в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-2582)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\SwInit.exe (11.5.0.595)
localhost	23715	Высокий	Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1286)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23716	Высокий	Множественные повреждения памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1284)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23219	Высокий	Уязвимость DoS в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-2581)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	23192	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2864)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5

localhost	23193	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2863)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	64343	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0574)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	64342	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0573)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	58121	Высокий	Adobe Flash Player до 13.0.0.250 и 14.x и 15.x до 15.0.0.189, Adobe AIR до 15.0.0.293 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) (CVE-2014-0558)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	23720	Высокий	Уязвимость в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1280)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23190	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2866)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	58122	Высокий	Adobe Flash Player до 13.0.0.250 и 14.x и 15.x до 15.0.0.189, Adobe AIR до 15.0.0.293 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) (CVE-2014-0564)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	58123	Высокий	Adobe Flash Player до 13.0.0.250 и 14.x и 15.x до 15.0.0.189, Adobe AIR до 15.0.0.293 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) (CVE-2014-0569)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	64348	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0583)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	64349	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0583)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	64346	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0581)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	23766	Высокий	Переполнение кучи в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-0987)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23767	Высокий	Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-0986)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	64347	Высокий	Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0582)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe

			AIR!DisplayVersion:15.0.0.249
localhost	23717	Высокий	Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1283)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56103	Высокий	Переполнение буфера в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2012-4175)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56104	Высокий	Переполнение буфера в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2012-4174)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56105	Высокий	Переполнение буфера в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2012-4173)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56110	Высокий	Повреждение памяти в Adobe Shockwave Player (CVE-2013-0635)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56111	Высокий	Переполнение буфера в Adobe Shockwave Player (CVE-2013-0636)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56106	Высокий	Переполнение буфера в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2012-4172)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56085	Высокий	Повреждение памяти в Adobe Shockwave Player до версии 11.6.4.634 (CVE-2012-0759)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56082	Высокий	Повреждение памяти в Adobe Shockwave Player, связанное с библиотекой DIRapi (CVE-2011-2446)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56079	Высокий	Многочисленные повреждения памяти в Adobe Shockwave Player (CVE-2011-2449)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56094	Высокий	Повреждение памяти в Adobe Shockwave Player (CVE-2012-2031)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56083	Высокий	Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player (CVE-2012-0757)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56084	Высокий	Переполнение кучи в Adobe Shockwave Player до версии 11.6.4.634 (CVE-2012-0758)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56107	Высокий	Выход за границу массива в Adobe Shockwave Player (CVE-2012-4176)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23713	Высокий	Переполнение буфера в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1288)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave

Player!DisplayVersion:11.5

localhost	56099	Высокий	Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (III) (CVE-2012-2045)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56100	Высокий	Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (IV) (CVE-2012-2046)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23714	Высокий	Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1287)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23711	Высокий	Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1290)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23712	Высокий	Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1289)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56096	Высокий	Повреждение памяти в Adobe Shockwave Player (CVE-2012-2033)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56097	Высокий	Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2012-2043)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56102	Высокий	Переполнение буфера в Adobe Shockwave Player до версии 11.6.7.638 посредством неопределённых векторов атаки (CVE-2012-5273)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56101	Высокий	Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (V) (CVE-2012-2047)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56098	Высокий	Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (II) (CVE-2012-2044)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56095	Высокий	Повреждение памяти в Adobe Shockwave Player (CVE-2012-2032)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	22969	Высокий	Повреждение памяти в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-4085)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	31248	Высокий	Переполнение кучи в Adobe Shockwave Player до 11.5.6.606 (CVE-2009-4002)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	31254	Высокий	Уязвимость в Adobe Shockwave Player до 11.5.2.602 (CVE-2009-3466)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	31255	Высокий	Уязвимость в Adobe Shockwave Player до 11.5.2.602 (CVE-2009-3465)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5

localhost	64287	Высокий	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.2.0.2 (CVE-2012-0519)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	64304	Высокий	Уязвимость в TNS Listener в Oracle Database 11g 11.1.0.7, 11.2.0.2 и 11.2.0.3 и 10g 10.2.0.3, 10.2.0.4 и 10.2.0.5 (CVE-2012-1675)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	64276	Высокий	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-2253)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	64350	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0585)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	23180	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2876)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23181	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2875)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	31221	Высокий	Множественные целочисленные переполнения в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-0129)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	31222	Высокий	Ошибка знаковости в dirapi.dll в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-0128)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	31223	Высокий	Уязвимость в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-0127)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	64270	Высокий	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-2239)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	64357	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-8440)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	64356	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-8438)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	64354	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0590)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	64351	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0586)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249

localhost	64352	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0588)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	31256	Высокий	Уязвимость в Adobe Shockwave Player до 11.5.2.602 (CVE-2009-3464)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	64359	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-8442)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	64294	Высокий	Неопределённая уязвимость в Oracle Spatial компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-0552)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	31220	Высокий	Целочисленное переполнение в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-0130)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	64358	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-8441)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	31257	Высокий	Уязвимость в Adobe Shockwave Player до 11.5.2.602 (CVE-2009-3463)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	64353	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0589)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	23182	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2874)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	19545	Высокий	Уязвимость, связанная с обходом проверки подлинности LDAPS (CVE-2011-2014)
cpe:/o:microsoft:windows_7::sp1:x64			C:\Windows\System32\ntdsai.dll (6.1.7600.17232)
localhost	19549	Высокий	Уязвимость в Active Directory, связанная с переполнением буфера (CVE-2011-3406)
cpe:/o:microsoft:windows_7::sp1:x64			C:\Windows\System32\ntdsai.dll (6.1.7600.17232)
localhost	21340	Высокий	Уязвимость целочисленного переполнения в Adobe Shockwave Player (CVE-2009-4003)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	22965	Высокий	Уязвимость в IML32.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-4089)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\iml32.dll (11.5.0.595)
localhost	22966	Высокий	Уязвимость в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-4088)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	22963	Высокий	Уязвимость доступа к освобожденной памяти в Adobe Shockwave Player 11.5.9.620 и ниже (CVE-2010-4092)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\Swinit.exe (11.5.0.595)



localhost	22970	Высокий	Уязвимость DoS в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-4084)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	22967	Высокий	Уязвимость DoS в IML32.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-4087)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\iml32.dll (11.5.0.595)
localhost	22968	Высокий	Уязвимость DoS в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-4086)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	23048	Высокий	Переполнение стека в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-3655)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	23049	Высокий	Повреждение памяти в Director модуле (dirapi.dll) Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-3653)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	23174	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2882)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	22964	Высокий	Уязвимость в Adobe Shockwave Player 11.5.9.615 и ниже позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки (CVE-2010-4090)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)
localhost	23178	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2878)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23187	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2869)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23188	Высокий	Множественные уязвимости в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2868)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23179	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2877)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23176	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2880)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23177	Высокий	Уязвимость целочисленного переполнения в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2879)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23184	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2872)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	23185	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2871)

<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	23175	<b>Высокий</b>	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2881)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	23189	<b>Высокий</b>	Уязвимость смещения указателя в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2867)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	23186	<b>Высокий</b>	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2870)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	23183	<b>Высокий</b>	Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2873)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56080	<b>Высокий</b>	Повреждение памяти в Adobe Shockwave Player, связанное с библиотекой DIRapi (CVE-2011-2448)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56026	<b>Высокий</b>	Целочисленное переполнение в компоненте CursorAsset x32 в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2120)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)</i>
localhost	56023	<b>Высокий</b>	Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2124)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)</i>
localhost	56024	<b>Высокий</b>	Целочисленное переполнение в компоненте Shockwave 3D Asset x32 в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2123)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)</i>
localhost	56027	<b>Высокий</b>	Уязвимость, связанная с удалённым выполнением кода в компоненте FLV ASSET Xtra в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2118)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)</i>
localhost	56028	<b>Высокий</b>	Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2117)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)</i>
localhost	56029	<b>Высокий</b>	Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2114)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)</i>
localhost	56069	<b>Высокий</b>	Уязвимость класса input validation в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4193)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56066	<b>Высокий</b>	Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4190)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56063	<b>Высокий</b>	Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4187)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56025	<b>Высокий</b>	Целочисленное переполнение в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2121)

<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\SwInit.exe (11.5.0.595)</i>
localhost	56067	Высокий	Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4191)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56068	Высокий	Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4192)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56022	Высокий	Переполнение буфера в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2126)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\SwInit.exe (11.5.0.595)</i>
localhost	56041	Высокий	Уязвимость, связанная с удалённым выполнением кода в IML32.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2115)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\iml32.dll (11.5.0.595)</i>
localhost	56030	Высокий	Многочисленное переполнение буфера в компоненте Shockwave3DAsset в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2113)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\SwInit.exe (11.5.0.595)</i>
localhost	56019	Высокий	Отказ в обслуживании в Adobe Shockwave Player (CVE-2013-1386)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56042	Высокий	Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2116)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\iml32.dll (11.5.0.595)</i>
localhost	56039	Высокий	Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2111)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\iml32.dll (11.5.0.595)</i>
localhost	56040	Высокий	Переполнение буфера в модуле TextXtra.x32 в IML32.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2112)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\iml32.dll (11.5.0.595)</i>
localhost	31259	Высокий	Уязвимость в Adobe Shockwave Player до 11.5.2.602 (CVE-2009-3244)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56016	Высокий	Переполнение буфера в Adobe Shockwave Player (CVE-2013-1383)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56017	Высокий	Отказ в обслуживании в Adobe Shockwave Player (CVE-2013-1384)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56020	Высокий	Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2128)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\SwInit.exe (11.5.0.595)</i>
localhost	56021	Высокий	Удалённое повреждение памяти в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2127)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\SwInit.exe (11.5.0.595)</i>
localhost	56018	Высокий	Уязвимость открытого доступа к информации в Adobe Shockwave Player (CVE-2013-1385)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56064	Высокий	Отказ в обслуживании (повреждение памяти) в модуле dirapi.dll of Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4188)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)</i>

localhost	56048	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player (CVE-2013-5333)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56054	Высокий	Уязвимость, связанная с удалённым выполнением кода в msvcr90.dll в Adobe Shockwave Player (CVE-2011-2423)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)
localhost	56059	Высокий	Отказ в обслуживании (повреждение памяти) в модуле dirapi.dll в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-2587)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	56049	Высокий	Уязвимость повреждения памяти в Adobe Shockwave Player (CVE-2013-5334)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56046	Высокий	Повреждение памяти в Adobe Shockwave Player (CVE-2013-3359)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56047	Высокий	Повреждение памяти в Adobe Shockwave Player (CVE-2013-3360)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56055	Высокий	Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player (CVE-2011-2420)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)
localhost	56056	Высокий	Уязвимость, связанная с удалённым выполнением кода в компоненте IML32.dll в Adobe Shockwave Player (CVE-2011-2419)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\iml32.dll (11.5.0.595)
localhost	56057	Высокий	Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player (i) (CVE-2010-4309)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)
localhost	56060	Высокий	Отказ в обслуживании (повреждение памяти) в модуле dirapi.dll of Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-2588)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	56061	Высокий	Целочисленное переполнение в модуле dirapi.dll в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-2589)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	56058	Высокий	Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player (ii) (CVE-2010-4308)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)
localhost	56053	Высокий	Уязвимость, связанная с удалённым выполнением кода в Dirapi.dll в Adobe Shockwave Player через специально сформированный .dir медиафайл (CVE-2011-2421)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	56076	Высокий	Целочисленное переполнение в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2011-0557)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56077	Высокий	Отказ в обслуживании (повреждение памяти) в модуле Font Xtra.x32 в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2011-0569)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56074	Высокий	Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2011-0555)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5

localhost	56065	Высокий	Отказ в обслуживании (повреждение памяти) в модуле IML32 в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4189)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\iml32.dll (11.5.0.595)
localhost	56070	Высокий	Уязвимость класса input validation в модуле dirapi.dll в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4194)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	56075	Высокий	Отказ в обслуживании (повреждение памяти) в модуле Font Xtra.x32 в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2011-0556)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56062	Высокий	Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4093)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56050	Высокий	Неопределённая уязвимость в Adobe Shockwave Player (CVE-2009-1860)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)
localhost	56052	Высокий	Уязвимость, связанная с удалённым выполнением кода в компоненте Textra.x32 в Adobe Shockwave Player (CVE-2011-2422)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)
localhost	56071	Высокий	Уязвимость класса input validation в модуле TextXtra в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4195)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56072	Высокий	Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4306)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56073	Высокий	Переполнение буфера в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4307)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56045	Высокий	Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2013-3348)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	72091	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3078)
cpe:/a:adobe:adobe_air			C:\Windows\system32\Macromed\Flash\Fish64_17_0_0_169.ocx (17.0.0.169)
cpe:/a:adobe:flash_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169
cpe:/a:adobe:shockwave_flash_activex			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FishPlayerPlugin!Version:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FishPlayerActiveX!Version:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	72101	Высокий	Уязвимость переполнения кучи в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3088)
cpe:/a:adobe:adobe_air			C:\Windows\system32\Macromed\Flash\Fish64_17_0_0_169.ocx (17.0.0.169)
cpe:/a:adobe:flash_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169
cpe:/a:adobe:shockwave_flash_activex			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FishPlayerPlugin!Version:17.0.0.169

HKEY\_LOCAL\_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249

localhost	72102	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3089)
cpe:/a:adobe:adobe_air			C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)
cpe:/a:adobe:flash_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169
cpe:/a:adobe:shockwave_flash_activex			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	69497	Высокий	Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 позволяет (CVE-2015-0459)
cpe:/a:oracle:jre:1.8.0			C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26) C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
localhost	69503	Высокий	Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0460)
cpe:/a:oracle:jre:1.8.0			C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26) C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
localhost	69504	Высокий	Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0469)
cpe:/a:oracle:jre:1.8.0			C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26) C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
localhost	72097	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3084)
cpe:/a:adobe:adobe_air			C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)
cpe:/a:adobe:flash_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169
cpe:/a:adobe:shockwave_flash_activex			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	72099	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3086)
cpe:/a:adobe:adobe_air			C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)
cpe:/a:adobe:flash_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169
cpe:/a:adobe:shockwave_flash_activex			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	69496	Высокий	Неопределённая уязвимость в в Oracle Java SE 6u91, 7u76, и 8u40 (CVE-2015-0458)
cpe:/a:oracle:jre:1.8.0			C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26) C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
localhost	72103	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3090)

cpe:/a:adobe:adobe_air		C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)	
cpe:/a:adobe:flash_player		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169	
cpe:/a:adobe:shockwave_flash_activex		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169	
		HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169	
		HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169	
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249	
localhost	72100	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3087)
cpe:/a:adobe:adobe_air		C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)	
cpe:/a:adobe:flash_player		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169	
cpe:/a:adobe:shockwave_flash_activex		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169	
		HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169	
		HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169	
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249	
localhost	72093	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3080)
cpe:/a:adobe:adobe_air		C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)	
cpe:/a:adobe:flash_player		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169	
cpe:/a:adobe:shockwave_flash_activex		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169	
		HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169	
		HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169	
		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249	
localhost	69514	Высокий	Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0491)
cpe:/a:oracle:jre:1.8.0		C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)	
		C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)	
localhost	56092	Высокий	Повреждение памяти в Adobe Shockwave Player (CVE-2012-2029)
cpe:/a:adobe:shockwave_player		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5	
localhost	56093	Высокий	Повреждение памяти в Adobe Shockwave Player (CVE-2012-2030)
cpe:/a:adobe:shockwave_player		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5	
localhost	56090	Высокий	Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player (CVE-2012-0764)
cpe:/a:adobe:shockwave_player		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5	
localhost	56081	Высокий	Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2011-2447)
cpe:/a:adobe:shockwave_player		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5	
localhost	56086	Высокий	Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player до версии 11.6.4.634 (CVE-2012-0760)
cpe:/a:adobe:shockwave_player		HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5	
localhost	56091	Высокий	Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player (CVE-2012-0766)

<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	69515	Высокий	Неопределённая уязвимость в Oracle Java SE 7u76 и 8u40 (CVE-2015-0492)
<i>cpe:/a:oracle:jre:1.8.0</i>			<i>C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)</i> <i>C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)</i>
localhost	72047	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3093)
<i>cpe:/a:adobe:adobe_air</i>			<i>C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)</i>
<i>cpe:/a:adobe:flash_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169</i>
<i>cpe:/a:adobe:shockwave_flash_activex</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169</i>
			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169</i>
			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169</i>
			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249</i>
localhost	72090	Высокий	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3077)
<i>cpe:/a:adobe:adobe_air</i>			<i>C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)</i>
<i>cpe:/a:adobe:flash_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169</i>
<i>cpe:/a:adobe:shockwave_flash_activex</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169</i>
			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169</i>
			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169</i>
			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249</i>
localhost	56087	Высокий	Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player (CVE-2012-0761)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56088	Высокий	Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player (CVE-2012-0762)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	56089	Высокий	Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player (CVE-2012-0763)
<i>cpe:/a:adobe:shockwave_player</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5</i>
localhost	63825	Высокий	Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) (CVE-2015-0306)
<i>cpe:/a:adobe:adobe_air</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249</i>
localhost	56036	Высокий	Удалённое повреждение памяти в модуле dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-0318)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)</i>
localhost	56037	Высокий	Уязвимость, связанная с удалённым выполнением кода в модуле dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-0320)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)</i>
localhost	56034	Высокий	Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2119)
<i>cpe:/a:adobe:shockwave_player</i>			<i>C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)</i>



localhost	43544	Высокий	Неопределённая уязвимость в Workload Manager компоненте в Oracle Database Server 11.2.0.2 и 11.2.0.3 (CVE-2013-1534)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	56078	Высокий	Уязвимость класса input validation, связанная с удалённым выполнением кода в модуле Shockwave 3D assets в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4196)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	56035	Высокий	Уязвимость, связанная с удалённым выполнением кода в модуле dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-0317)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	56038	Высокий	Уязвимость, связанная с удалённым выполнением кода в модуле dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-0335)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	56043	Высокий	Уязвимость, связанная с удалённым выполнением кода в модуле dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-0319)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	56044	Высокий	Переполнение буфера в модуле Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2125)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)
localhost	56031	Высокий	Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2108)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)
localhost	56032	Высокий	Целочисленное переполнение в Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2109)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	56033	Высокий	Удалённое повреждение памяти в Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2122)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\dirapi.dll (11.5.0.595)
localhost	43543	Высокий	Неопределённая уязвимость в Oracle executable компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2013-3771)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	63830	Высокий	Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows не правильно проверяет файлы, что имеет неопределённое воздействие на систему (CVE-2015-0301)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	63828	Высокий	Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) (CVE-2015-0303)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	63827	Высокий	Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленникам выполнить произвольный код (CVE-2015-0304)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	63824	Высокий	Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленнику получить доступ к конфиденциальной информации (CVE-2015-0307)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249

localhost	63823	Высокий	Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленнику выполнить произвольный код (CVE-2015-0308)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	63826	Высокий	Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленникам выполнить произвольный код (CVE-2015-0305)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	43587	Высокий	Уязвимость в Adobe Shockwave Player до 12.0.9.149 (CVE-2014-0500)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)
localhost	43545	Высокий	Неопределённая уязвимость в Oracle executable компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2013-3760)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	43535	Высокий	Уязвимость в Adobe Shockwave Player до 12.0.9.149 (CVE-2014-0501)
cpe:/a:adobe:shockwave_player			C:\Windows\syswow64\Adobe\Shockwave 11\Swlnit.exe (11.5.0.595)
localhost	63822	Высокий	Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленнику выполнить произвольный код (CVE-2015-0309)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	43548	Высокий	Неопределённая уязвимость в XML Parser компоненте в Oracle Database Server 11.2.0.2 и 11.2.0.3 (CVE-2013-3751)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	43551	Высокий	Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2013-3774)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	64242	Средний	Неопределённая уязвимость в Oracle Help компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1, 11.2.0.2, 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5 и 10.1.0.5 (CVE-2011-0785)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	23718	Средний	Уязвимость в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1282)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	53418	Средний	Уязвимость Microsoft SQL Server, приводящая к переполнению стека (CVE-2014-4061)
cpe:/a:microsoft:sql_server:2012			C:\Program Files\Microsoft SQL Server\110\Setup Bootstrap\SQLServer2012\x64\Microsoft.SqlServer.Chainer.Infrastructure.dll (11.0.3128.0)
localhost	64355	Средний	Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-8437)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	64255	Средний	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0835)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	64253	Средний	Неопределённая уязвимость в Enterprise Config Management компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0831)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All

localhost	43542	Средний	Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2013-1554)
cpe:/a:oracle:database_server			Versions\1\Version:11.2.0.2.0 HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64254	Средний	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0832)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64251	Средний	Неопределённая уязвимость в CMDDB Metadata & Instance APIs компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0816)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64249	Средний	Неопределённая уязвимость в Network Foundation компоненте в Oracle Database Server 10.1.0.5, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0806)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64281	Средний	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 и 11.2.0.2 (CVE-2011-3512)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64282	Средний	Неопределённая уязвимость в Listener компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 и 11.2.0.2 (CVE-2012-0072)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64257	Средний	Неопределённая уязвимость в Security Framework компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0848)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64260	Средний	Неопределённая уязвимость в Enterprise Manager Console компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0876)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	23191	Средний	Уязвимость в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2865)
cpe:/a:adobe:shockwave_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Shockwave Player!DisplayVersion:11.5
localhost	64256	Средний	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0838)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	53417	Средний	Уязвимость SQL Master Data Services, приводящая к межсайтовому выполнению сценариев (XSS) (CVE-2014-1820)
cpe:/a:microsoft:sql_server:2012			C:\Program Files\Microsoft SQL Server\110\Setup Bootstrap\SQLServer2012\x64\Microsoft.SqlServer.Chainer.Infrastructure.dll (11.0.3128.0)
localhost	64275	Средний	Неопределённая уязвимость в SQL Performance Advisories/UIs компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-2248)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64277	Средний	Неопределённая уязвимость в Database Target Type Menus компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-2257)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All

Versions\1\Version:11.2.0.2.0

localhost	64289	Средний	Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-0525)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64286	Средний	Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 11.1.0.7 и 11.2.0.2 (CVE-2012-0512)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64298	Средний	Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-1747)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64288	Средний	Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 и 11.2.0.2 (CVE-2012-0520)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	63829	Средний	Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленнику получить доступ к конфиденциальной информации (CVE-2015-0302)
cpe:/a:adobe:adobe_air			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	32978	Средний	Неопределённая уязвимость в XML Parser компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2, 11.2.0.3, и 12.1.0.1 (CVE-2013-5771)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64291	Средний	Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-0527)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64283	Средний	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-0082)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64290	Средний	Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-0526)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	72105	Средний	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3092)
cpe:/a:adobe:adobe_air			C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)
cpe:/a:adobe:flash_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169
cpe:/a:adobe:shockwave_flash_activex			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169 HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlexPlayerPlugin!Version:17.0.0.169 HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlexPlayerActiveX!Version:17.0.0.169 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	32981	Средний	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2, 11.2.0.3, и 12.1.0.1 (CVE-2013-3826)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All

localhost	64293	Средний	Неопределённая уязвимость в RDBMS Core компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-0534)
cpe:/a:oracle:database_server			Versions\1\Version:11.2.0.2.0 HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64295	Средний	Неопределённая уязвимость в Enterprise Manager для Oracle Database компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-1737)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64296	Средний	Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-1745)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	43536	Средний	Уязвимость в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2012-3137)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	43595	Средний	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2013-3789)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64297	Средний	Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-1746)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64299	Средний	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-1751)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	43591	Средний	Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 11.2.0.2 и 11.2.0.3 (CVE-2013-1538)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	64262	Средний	Неопределённая уязвимость в Instance Management компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0879)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1\Version:11.2.0.2.0
localhost	65601	Средний	Уязвимость в WCCP диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 (CVE-2015-0560)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	65603	Средний	Множественные уязвимости доступа к освобожденной памяти в DEC DNA Routing Protocol диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 (CVE-2015-0562)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	65597	Средний	Уязвимость в NCP диссекторе Wireshark 1.10.x до 1.10.11 и 1.12.x до 1.12.2 (CVE-2014-8712)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	65598	Средний	Переполнение стека в NCP диссекторе Wireshark 1.10.x до 1.10.11 и 1.12.x до 1.12.2 (CVE-2014-8713)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1

localhost	65604	Средний	Уязвимость в SMTP диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 (CVE-2015-0563)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	72094	Средний	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3081)
cpe:/a:adobe:adobe_air			C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)
cpe:/a:adobe:flash_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169
cpe:/a:adobe:shockwave_flash_activex			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	72095	Средний	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3082)
cpe:/a:adobe:adobe_air			C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)
cpe:/a:adobe:flash_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169
cpe:/a:adobe:shockwave_flash_activex			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169
			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	65602	Средний	Уязвимость в LPP диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 (CVE-2015-0561)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	58893	Средний	Уязвимость в SSL 3.0 (POODLE) в Internet Explorer (GPO) (CVE-2014-3566)
cpe:/o:microsoft:windows			
localhost	65600	Средний	Множественные уязвимости доступа к освобожденной памяти в WCCP диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 (CVE-2015-0559)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	65605	Средний	Незаполнение буфера в Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 (CVE-2015-0564)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	66678	Средний	Уязвимость в Wireshark 1.10.x до 1.10.13 и 1.12.x до 1.12.4 (CVE-2015-2188)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	66679	Средний	Уязвимость в в Wireshark 1.10.x до 1.10.13 и 1.12.x до 1.12.4 (CVE-2015-2189)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	66677	Средний	Уязвимость в Wireshark 1.12.x до 1.12.4 (CVE-2015-2187)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	66681	Средний	Уязвимость в Wireshark 1.10.x до 1.10.13 и 1.12.x до 1.12.4 (CVE-2015-2191)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	66682	Средний	Уязвимость в Wireshark 1.12.x до 1.12.4 (CVE-2015-2192)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1

sion:1.12.1

localhost	65599	Средний	Уязвимость в TN5250 диссекторе Wireshark 1.10.x до 1.10.11 и 1.12.x до 1.12.2 (CVE-2014-8714)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	66680	Средний	Уязвимость в Wireshark 1.12.x до 1.12.4 (CVE-2015-2190)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	65596	Средний	Множественные целочисленные переполнения в AMQP диссекторе Wireshark 1.10.x до 1.10.11 и 1.12.x до 1.12.2 (CVE-2014-8711)
cpe:/a:wireshark:wireshark			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark!DisplayVersion:1.12.1
localhost	69512	Средний	Неопределённая уязвимость в Oracle Java SE 8u40 (CVE-2015-0486)
cpe:/a:oracle:jre:1.8.0			C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26) C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
localhost	69513	Средний	Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0488)
cpe:/a:oracle:jre:1.8.0			C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26) C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
localhost	64301	Средний	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-3134)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	69507	Средний	Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0478)
cpe:/a:oracle:jre:1.8.0			C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26) C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
localhost	69509	Средний	Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0480)
cpe:/a:oracle:jre:1.8.0			C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26) C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
localhost	64263	Средний	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0880)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	64274	Средний	Неопределённая уязвимость в Security Framework компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-2244)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	69511	Средний	Неопределённая уязвимость в Oracle Java SE 7u76 и 8u40 (CVE-2015-0484)
cpe:/a:oracle:jre:1.8.0			C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26) C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
localhost	58892	Средний	Уязвимость в SSL 3.0 (POODLE) в Windows (CVE-2014-3566)
cpe:/o:microsoft:windows			
localhost	64300	Средний	Узвимость внедрения SQL в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-3132)
cpe:/a:oracle:database_server			HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	72096	Средний	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3083)
cpe:/a:adobe:adobe_air			C:\Windows\system32\Macromed\Flash\Fish64_17_0_0_169.ocx (17.0.0.169)
cpe:/a:adobe:flash_player			HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player

			ActiveX!DisplayVersion:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	20373	Средний	Уязвимость, приводящая к потреблению большого объема памяти (CVE-2013-1282)
			C:\Windows\System32\ntdsai.dll (6.1.7600.17232)
			HKKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	64306	Средний	Неопределённая уязвимость в Schema Management компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0870)
			HKKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0
localhost	72092	Средний	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3079)
			C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)
			HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	72104	Средний	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3091)
			C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)
			HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249
localhost	69505	Средний	Неопределённая уязвимость в Oracle Java SE 8u40 (CVE-2015-0470)
			C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
			C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
localhost	69506	Средний	Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0477)
			C:\Program Files (x86)\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
			C:\Program Files\Java\jre1.8.0_40\bin\java.exe (8.0.40.26)
localhost	72098	Средний	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3085)
			C:\Windows\system32\Macromed\Flash\Flash64_17_0_0_169.ocx (17.0.0.169)
			HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player ActiveX!DisplayVersion:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe Flash Player NPAPI!DisplayVersion:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerPlugin!Version:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\FlashPlayerActiveX!Version:17.0.0.169
			HKKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Adobe AIR!DisplayVersion:15.0.0.249



localhost	22840	Средний	Уязвимость обхода безопасности в Microsoft Windows Human Interface Device (HID) драйвере (CVE-2011-0638)
<i>cpe:/o:microsoft:windows</i>			<i>Служба: Доступ к HID-устройствам (SERVICE_RUNNING)</i>
localhost	64272	Низкий	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.2.0.1 и 11.2.0.2 (CVE-2011-2242)
<i>cpe:/a:oracle:database_server</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0</i>
localhost	64280	Низкий	Неопределённая уязвимость в Database Vault компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 и 11.2.0.2 (CVE-2011-3511)
<i>cpe:/a:oracle:database_server</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0</i>
localhost	64273	Низкий	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7.3, 11.2.0.1 и 11.2.0.2 (CVE-2011-2243)
<i>cpe:/a:oracle:database_server</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0</i>
localhost	64302	Низкий	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-3146)
<i>cpe:/a:oracle:database_server</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0</i>
localhost	43549	Низкий	Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2013-3790)
<i>cpe:/a:oracle:database_server</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0</i>
localhost	64247	Низкий	Неопределённая уязвимость в Database Vault компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0804)
<i>cpe:/a:oracle:database_server</i>			<i>HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\OracleMTSRecoveryService\Setup\All Versions\1!Version:11.2.0.2.0</i>

## Список уязвимостей

<b>Уязвимость</b>	Риск: Высокий
<b>ALTX ID</b> 56057	<b>Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player (i) (CVE-2010-4309)</b>
<b>Описание</b>	Adobe Shockwave Player до версии 11.6.1.629 и is prone to a Уязвимость, связанная с удалённым выполнением кода.
<b>Исправление</b>	Необходимо установить актуальное обновление от производителя.
<b>Ссылки</b>	<b>oval:ru.altx-soft.win:def:29323</b> <a href="http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29323">http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29323</a> <b>CVE-2010-4309 (CVE)</b> CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) CWE: CWE-119 <a href="#">CVE-2010-4309</a>

<b>Уязвимость</b>	Риск: Высокий
<b>ALTX ID</b> 56056	<b>Уязвимость, связанная с удалённым выполнением кода в компоненте IML32.dll в Adobe Shockwave Player (CVE-2011-2419)</b>
<b>Описание</b>	Adobe Shockwave Player до версии 11.6.1.629 и is prone to Уязвимость, связанная с удалённым выполнением кода. A flaw is present в IML32.dll, что fails to validate user supplied input. Successful exploitation could позволяет злоумышленникам выполнить произвольный код от падение the service.
<b>Исправление</b>	Необходимо установить актуальное обновление от производителя.
<b>Ссылки</b>	<b>oval:ru.altx-soft.win:def:29322</b> <a href="http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29322">http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29322</a> <b>CVE-2011-2419 (CVE)</b> CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C) CWE: CWE-119 <a href="#">CVE-2011-2419</a>

<b>Уязвимость</b>	Риск: Высокий
<b>ALTX ID</b> 56055	<b>Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player (CVE-2011-2420)</b>
<b>Описание</b>	Adobe Shockwave Player до версии 11.6.1.629 позволяет злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.
<b>Исправление</b>	Необходимо установить актуальное обновление от производителя.
<b>Ссылки</b>	

oval:ru.altx-soft.win:def:29321

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29321>

**CVE-2011-2420 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2420](#)

Уязвимость

Риск: Высокий

ALT X ID  
56058

**Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player (ii) (CVE-2010-4308)**

**Описание**

IML32.dll инв Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:29324

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29324>

**CVE-2010-4308 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4308](#)

Уязвимость

Риск: Высокий

ALT X ID  
56061

**Целочисленное переполнение в модуле dirapi.dll в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-2589)**

**Описание**

Модуль dirapi.dll of Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:29327

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29327>

**CVE-2010-2589 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2010-2589](#)

Уязвимость

Риск: Высокий

ALT X ID  
56060

**Отказ в обслуживании (повреждение памяти) в модуле dirapi.dll of Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-2588)**

**Описание**

Модуль dirapi.dll of Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить

произвольный код или вызвать отказ в обслуживании.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29326

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29326>

#### CVE-2010-2588 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2588](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
56059

**Отказ в обслуживании (повреждение памяти) в модуле dirapi.dll в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-2587)**

#### Описание

Отказ в обслуживании (повреждение памяти) в модуле dirapi.dll в Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании посредством неопределённых векторов.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29325

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29325>

#### CVE-2010-2587 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2587](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
56054

**Уязвимость, связанная с удалённым выполнением кода в msvcr90.dll в Adobe Shockwave Player (CVE-2011-2423)**

#### Описание

msvcr90.dll в Adobe Shockwave Player позволяет злоумышленникам выполнить произвольный код.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29320

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29320>

#### CVE-2011-2423 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2423](#)

#### Уязвимость

Риск: Высокий

ALTX ID

56048

## Уязвимость повреждения памяти в Adobe Shockwave Player (CVE-2013-5333)

### Описание

Adobe Shockwave Player до 12.0.7.148 позволяет удаленным злоумышленникам выполнить произвольный код или отказ в обслуживании.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:29314

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29314>

### CVE-2013-5333 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2013-5333](#)

Уязвимость

Риск: Высокий

ALTX ID

56047

## Повреждение памяти в Adobe Shockwave Player (CVE-2013-3360)

### Описание

Adobe Shockwave Player до 12.0.4.144 позволяет удаленным злоумышленникам выполнить произвольный код или отказ в обслуживании.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:29313

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29313>

### CVE-2013-3360 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2013-3360](#)

Уязвимость

Риск: Высокий

ALTX ID

56046

## Повреждение памяти в Adobe Shockwave Player (CVE-2013-3359)

### Описание

Adobe Shockwave Player до 12.0.4.144 позволяет удаленным злоумышленникам выполнить произвольный код или отказ в обслуживании.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:29312

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29312>

**CVE-2013-3359 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2013-3359](#)**Уязвимость**

Риск: Высокий

**ALT X ID**

56049

**Уязвимость повреждения памяти в Adobe Shockwave Player (CVE-2013-5334)****Описание**

Adobe Shockwave Player до 12.0.7.148 позволяет удаленным злоумышленникам выполнить произвольный код или отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29315**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29315>**CVE-2013-5334 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2013-5334](#)**Уязвимость**

Риск: Высокий

**ALT X ID**

56053

**Уязвимость, связанная с удалённым выполнением кода в Dirapi.dll в Adobe Shockwave Player через специально сформированный .dir медиафайл (CVE-2011-2421)****Описание**

Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29319**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29319>**CVE-2011-2421 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2421](#)**Уязвимость**

Риск: Высокий

**ALT X ID**

56052

**Уязвимость, связанная с удалённым выполнением кода в компоненте Textra.x32 в Adobe Shockwave Player (CVE-2011-2422)****Описание**

Уязвимость, связанная с удалённым выполнением кода в компоненте Textra.x32 в Adobe Shockwave Player до версии 11.6.1.629 позволяет удаленным злоумышленникам выполнить произвольный код.

**Исправление**

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29318

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29318>

#### CVE-2011-2422 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2422](#)

#### Уязвимость

Риск: Высокий

ALT X ID  
56050

**Неопределённая уязвимость в Adobe Shockwave Player (CVE-2009-1860)**

#### Описание

Adobe Shockwave Player до версии 11.5.0.600 позволяет удаленным злоумышленникам выполнить произвольный код посредством созданного Shockwave Player 10 контента.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29316

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29316>

#### CVE-2009-1860 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

[CVE-2009-1860](#)

#### Уязвимость

Риск: Высокий

ALT X ID  
56062

**Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4093)**

#### Описание

Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29328

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29328>

#### CVE-2010-4093 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4093](#)

#### Уязвимость

Риск: Высокий

ALT X ID  
56073

**Переполнение буфера в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4307)**

#### Описание

Переполнение буфера в Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

**oval:ru.altx-soft.win:def:29339**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29339>

**CVE-2010-4307 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4307](#)

Уязвимость

Риск: Высокий

ALTX ID

56072

**Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4306)**

#### Описание

Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать повреждение памяти.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

**oval:ru.altx-soft.win:def:29338**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29338>

**CVE-2010-4306 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4306](#)

Уязвимость

Риск: Высокий

ALTX ID

56071

**Уязвимость класса input validation в модуле TextXtra в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4195)**

#### Описание

Модуль TextXtra в Adobe Shockwave Player до 11.5.9.620 неправильно проверяет некоторые входные данные, что позволяет злоумышленникам выполнить произвольный код.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

**oval:ru.altx-soft.win:def:29337**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29337>

**CVE-2010-4195 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2010-4195](#)

Уязвимость

Риск: Высокий



ALTX ID

56074

**Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2011-0555)**

#### Описание

Модуль TextXtra.x32 в Adobe Shockwave Player до 11.5.9.620 неправильно проверяет некоторые входные данные, что позволяет злоумышленникам выполнить произвольный код.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29340

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29340>

#### CVE-2011-0555 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-0555](#)

Уязвимость

Риск: Высокий

ALTX ID

56077

**Отказ в обслуживании (повреждение памяти) в модуле Font Xtra.x32 в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2011-0569)**

#### Описание

Отказ в обслуживании (повреждение памяти) в модуле Font Xtra.x32 в Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29343

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29343>

#### CVE-2011-0569 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-0569](#)

Уязвимость

Риск: Высокий

ALTX ID

56076

**Целочисленное переполнение в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2011-0557)**

#### Описание

Целочисленное переполнение в Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29342

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29342>

**CVE-2011-0557 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2011-0557](#)**Уязвимость**

Риск: Высокий

**ALTX ID**

56075

**Отказ в обслуживании (повреждение памяти) в модуле Font Xtra.x32 в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2011-0556)****Описание**

Модуль Font Xtra.x32 в Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29341**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29341>**CVE-2011-0556 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-0556](#)**Уязвимость**

Риск: Высокий

**ALTX ID**

56070

**Уязвимость класса input validation в модуле dirapi.dll в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4194)****Описание**

Модуль dirapi.dll в Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29336**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29336>**CVE-2010-4194 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2010-4194](#)**Уязвимость**

Риск: Высокий

**ALTX ID**

56065

**Отказ в обслуживании (повреждение памяти) в модуле IML32 в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4189)****Описание**

Модуль IML32 в Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29331

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29331>

#### CVE-2010-4189 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4189](#)

#### Уязвимость

Риск: Высокий

ALT X ID  
56064

**Отказ в обслуживании (повреждение памяти) в модуле dirapi.dll of Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4188)**

#### Описание

Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29330

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29330>

#### CVE-2010-4188 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4188](#)

#### Уязвимость

Риск: Высокий

ALT X ID  
56063

**Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4187)**

#### Описание

Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29329

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29329>

#### CVE-2010-4187 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4187](#)

#### Уязвимость

Риск: Высокий

ALT X ID  
56066

**Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4190)**

### Описание

Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:29332**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29332>

### CVE-2010-4190 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4190](#)

### Уязвимость

Риск: Высокий

ALTX ID  
56069

**Уязвимость класса input validation в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4193)**

### Описание

Adobe Shockwave Player до версии 11.5.9.620 неправильно проверяет некоторые входные данные, что позволяет удаленным злоумышленникам выполнить произвольный код.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:29335**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29335>

### CVE-2010-4193 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2010-4193](#)

### Уязвимость

Риск: Высокий

ALTX ID  
56068

**Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4192)**

### Описание

Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать повреждение памяти.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:29334**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29334>

### CVE-2010-4192 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4192](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
56067**Отказ в обслуживании (повреждение памяти) в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4191)****Описание**

Adobe Shockwave Player до версии 11.5.9.620 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать повреждение памяти.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:29333

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29333>

**CVE-2010-4191 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4191](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
56025**Целочисленное переполнение в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2121)****Описание**

Целочисленное переполнение в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:29291

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29291>

**CVE-2011-2121 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2011-2121](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
56024**Целочисленное переполнение в компоненте Shockwave 3D Asset x32 в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2123)****Описание**

Целочисленное переполнение в компоненте Shockwave 3D Asset x32 в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код посредством специально созданной записи в DEMX, которая вызывает переполнение динамической памяти.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:29290

<http://www.ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29290>

**CVE-2011-2123 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2011-2123](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
56023

**Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2124)**

**Описание**

Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании посредством неопределённых векторов.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

**oval:ru.altx-soft.win:def:29289**

<http://www.ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29289>

**CVE-2011-2124 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2124](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
56026

**Целочисленное переполнение в компоненте CursorAsset x32 в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2120)**

**Описание**

Целочисленное переполнение в компоненте CursorAsset x32 в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

**oval:ru.altx-soft.win:def:29292**

<http://www.ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29292>

**CVE-2011-2120 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2011-2120](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
56029

**Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2114)**

**Описание**

Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании посредством неопределённых векторов.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29295

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29295>

#### CVE-2011-2114 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2114](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
56028

**Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2117)**

#### Описание

Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании посредством неопределённых векторов.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29294

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29294>

#### CVE-2011-2117 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2117](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
56027

**Уязвимость, связанная с удалённым выполнением кода в компоненте FLV ASSET Xtra в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2118)**

#### Описание

Уязвимость, связанная с удалённым выполнением кода в компоненте FLV ASSET Xtra в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29293

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29293>

#### CVE-2011-2118 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2011-2118](#)

#### Уязвимость

Риск: Высокий

ALTX ID

56022

## Переполнение буфера в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2126)

### Описание

Переполнение буфера в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код посредством неопределённых векторов.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:29288

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29288>

### CVE-2011-2126 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2126](#)

Уязвимость

Риск: Высокий

ALTX ID

56017

## Отказ в обслуживании в Adobe Shockwave Player (CVE-2013-1384)

### Описание

Adobe Shockwave Player до версии 12.0.2.122 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании посредством неопределённых векторов.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:29283

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29283>

### CVE-2013-1384 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2013-1384](#)

Уязвимость

Риск: Высокий

ALTX ID

56016

## Переполнение буфера в Adobe Shockwave Player (CVE-2013-1383)

### Описание

Переполнение буфера в Adobe Shockwave Player до версии 12.0.2.122 позволяет удаленным злоумышленникам выполнить произвольный код посредством неопределённых векторов.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:29282

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29282>



### CVE-2013-1383 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2013-1383](#)

Уязвимость

Риск: Высокий

ALT X ID

31259

**Уязвимость в Adobe Shockwave Player до 11.5.2.602 (CVE-2009-3244)**

Описание

Переполнение кучи в SwDir.dll ActiveX control в Adobe Shockwave Player 11.5.1.601 и ниже позволяет удалённым злоумышленникам вызвать отказ в обслуживании и выполнить произвольный код через длинное значение свойства PlayerVersion.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.win:def:27748

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:27748>

### CVE-2009-3244 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2009-3244](#)

Уязвимость

Риск: Высокий

ALT X ID

56018

**Уязвимость открытого доступа к информации в Adobe Shockwave Player (CVE-2013-1385)**

Описание

Adobe Shockwave Player до версии 12.0.2.122 не блокирует доступ к адресам, что облегчает злоумышленникам обойти механизм защиты ASLR посредством неопределённых векторов.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.win:def:29284

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29284>

### CVE-2013-1385 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-264

[CVE-2013-1385](#)

Уязвимость

Риск: Высокий

ALT X ID

56021

**Удалённое повреждение памяти в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2127)**

Описание

Adobe Shockwave Player до версии 11.6.0.626 позволяет удалённым злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании посредством неопределённых векторов.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29287

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29287>

#### CVE-2011-2127 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2127](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
56020

**Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2128)**

#### Описание

Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании посредством неопределённых векторов.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29286

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29286>

#### CVE-2011-2128 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2128](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
56019

**Отказ в обслуживании в Adobe Shockwave Player (CVE-2013-1386)**

#### Описание

Adobe Shockwave Player до версии 12.0.2.122 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании посредством неопределённых векторов.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29285

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29285>

#### CVE-2013-1386 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2013-1386](#)

#### Уязвимость

Риск: Высокий

ALTX ID

56030

**Многочисленное переполнение буфера в компоненте Shockwave3DAsset в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2113)**

#### Описание

Многочисленное переполнение буфера в компоненте Shockwave3DAsset в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29296

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29296>

#### CVE-2011-2113 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2113](#)

Уязвимость

Риск: Высокий

ALTX ID

56041

**Уязвимость, связанная с удалённым выполнением кода в IML32.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2115)**

#### Описание

IML32.dll inv Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29307

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29307>

#### CVE-2011-2115 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2115](#)

Уязвимость

Риск: Высокий

ALTX ID

56040

**Переполнение буфера в модуле TextXtra.x32 в IML32.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2112)**

#### Описание

Переполнение буфера в модуле TextXtra.x32 в IML32.dll в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29306

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29306>

**CVE-2011-2112 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2112](#)**Уязвимость**

Риск: Высокий

**ALTX ID**

56039

**Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2111)****Описание**

IML32.dll inv Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29305**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29305>**CVE-2011-2111 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2111](#)**Уязвимость**

Риск: Высокий

**ALTX ID**

56042

**Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2116)****Описание**

IML32.dll inv Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29308**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29308>**CVE-2011-2116 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2116](#)**Уязвимость**

Риск: Высокий

**ALTX ID**

56045

**Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2013-3348)****Описание**

Adobe Shockwave Player до версии 12.0.3.133 позволяет удаленным злоумышленникам выполнить произвольный код или вызывает повреждение памяти.

**Исправление**

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29311

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29311>

#### CVE-2013-3348 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2013-3348](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
56044

**Переполнение буфера в модуле Dirapix.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2125)**

#### Описание

Переполнение буфера в модуле Dirapix.dll в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29310

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29310>

#### CVE-2011-2125 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2125](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
56043

**Уязвимость, связанная с удалённым выполнением кода в модуле dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-0319)**

#### Описание

Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29309

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29309>

#### CVE-2011-0319 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-0319](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
56038

**Уязвимость, связанная с удалённым выполнением кода в модуле dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-0335)**

### Описание

Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:29304**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29304>

### CVE-2011-0335 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-0335](#)

### Уязвимость

Риск: Высокий

ALTX ID  
56033

**Удалённое повреждение памяти в Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2122)**

### Описание

Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:29299**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29299>

### CVE-2011-2122 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2122](#)

### Уязвимость

Риск: Высокий

ALTX ID  
56032

**Целочисленное переполнение в Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2109)**

### Описание

Целочисленное переполнение в Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:29298**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29298>

### CVE-2011-2109 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2011-2109](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
56031**Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2108)****Описание**

Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29297**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29297>**CVE-2011-2108 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

[CVE-2011-2108](#)**Уязвимость**

Риск: Высокий

ALTX ID  
56034**Уязвимость, связанная с удалённым выполнением кода в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-2119)****Описание**

Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29300**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29300>**CVE-2011-2119 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2119](#)**Уязвимость**

Риск: Высокий

ALTX ID  
56037**Уязвимость, связанная с удалённым выполнением кода в модуле dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-0320)****Описание**

Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29303**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29303>

### CVE-2011-0320 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-0320](#)

Уязвимость

Риск: Высокий

ALT X ID

56036

**Удалённое повреждение памяти в модуле dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-0318)**

Описание

Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.win:def:29302

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29302>

### CVE-2011-0318 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-0318](#)

Уязвимость

Риск: Высокий

ALT X ID

56035

**Уязвимость, связанная с удалённым выполнением кода в модуле dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 (CVE-2011-0317)**

Описание

Dirapi.dll в Adobe Shockwave Player до версии 11.6.0.626 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.win:def:29301

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29301>

### CVE-2011-0317 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-0317](#)

Уязвимость

Риск: Высокий

ALT X ID

56078

**Уязвимость класса input validation, связанная с удалённым выполнением кода in модуле Shockwave 3D assets в Adobe Shockwave Player до версии 11.5.9.620 (CVE-2010-4196)**

Описание

Модуль Shockwave 3D assets в Adobe Shockwave Player до версии 11.5.9.620 неправильно проверяет некоторые входные данные, что позволяет злоумышленникам выполнить произвольный код.

Исправление



Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29344

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29344>

#### CVE-2010-4196 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2010-4196](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
43544

**Неопределённая уязвимость в Workload Manager компоненте в Oracle Database Server 11.2.0.2 и 11.2.0.3 (CVE-2013-1534)**

#### Описание

Неопределённая уязвимость в Workload Manager компоненте в Oracle Database Server 11.2.0.2 и 11.2.0.3, при использовании Oracle RAC, позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:32439

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:32439>

#### CVE-2013-1534 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2013-1534](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
43543

**Неопределённая уязвимость в Oracle executable компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2013-3771)**

#### Описание

Неопределённая уязвимость в Oracle executable компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 позволяет локальным пользователям повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2013-3760.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:32438

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:32438>

#### CVE-2013-3771 (CVE)

CVSS: Базовая оценка 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2013-3771](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
43535

**Уязвимость в Adobe Shockwave Player до 12.0.9.149 (CVE-2014-0501)**

### Описание

Adobe Shockwave Player до 12.0.9.149 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0500.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:32430

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:32430>

### CVE-2014-0501 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2014-0501](#)

### Уязвимость

Риск: Высокий

ALTX ID  
43545

**Неопределённая уязвимость в Oracle executable компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2013-3760)**

### Описание

Неопределённая уязвимость в Oracle executable компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 позволяет локальным пользователям повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2013-3771.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:32440

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:32440>

### CVE-2013-3760 (CVE)

CVSS: Базовая оценка 7.2 (AV:L/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2013-3760](#)

### Уязвимость

Риск: Высокий

ALTX ID  
43587

**Уязвимость в Adobe Shockwave Player до 12.0.9.149 (CVE-2014-0500)**

### Описание

Adobe Shockwave Player до 12.0.9.149 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0501.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:32483

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:32483>

### CVE-2014-0500 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2014-0500](#)

Уязвимость

Риск: Высокий

ALTX ID

43551

**Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2013-3774)**

Описание

Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.win:def:32446

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:32446>

### CVE-2013-3774 (CVE)

CVSS: Базовая оценка 7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)

[CVE-2013-3774](#)

Уязвимость

Риск: Высокий

ALTX ID

43548

**Неопределённая уязвимость в XML Parser компоненте в Oracle Database Server 11.2.0.2 и 11.2.0.3 (CVE-2013-3751)**

Описание

Неопределённая уязвимость в XML Parser компоненте в Oracle Database Server 11.2.0.2 и 11.2.0.3 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.win:def:32443

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:32443>

### CVE-2013-3751 (CVE)

CVSS: Базовая оценка 9 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

[CVE-2013-3751](#)

Уязвимость

Риск: Высокий

ALTX ID

63822

**Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленнику выполнить произвольный код (CVE-2015-0309)**

Описание

Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленнику выполнить произвольный код посредством неопределённого вектора атаки.

Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:29544

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29544>

#### CVE-2015-0309 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2015-0309](#)

#### Уязвимость

Риск: Высокий

ALT X ID  
63827

**Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленникам выполнить произвольный код (CVE-2015-0304)**

#### Описание

Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленникам выполнить произвольный код посредством неопределённого вектора атаки.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:29539

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29539>

#### CVE-2015-0304 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2015-0304](#)

#### Уязвимость

Риск: Высокий

ALT X ID  
63828

**Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) (CVE-2015-0303)**

#### Описание

Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) посредством неопределённого вектора атаки.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:29538

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29538>

#### CVE-2015-0303 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2015-0303](#)

#### Уязвимость

Риск: Высокий

ALTX ID

63830

**Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows не правильно проверяет файлы, что имеет неопределенное воздействие на систему (CVE-2015-0301)**

#### Описание

Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows не правильно проверяет файлы, что имеет неопределенное воздействие на систему.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:29536

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29536>

#### CVE-2015-0301 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2015-0301](#)

Уязвимость

Риск: Высокий

ALTX ID

63826

**Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленникам выполнить произвольный код (CVE-2015-0305)**

#### Описание

Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленникам выполнить произвольный код посредством неопределённого вектора атаки.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:29540

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29540>

#### CVE-2015-0305 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

[CVE-2015-0305](#)

Уязвимость

Риск: Высокий

ALTX ID

63823

**Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленнику выполнить произвольный код (CVE-2015-0308)**

#### Описание

Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленнику выполнить произвольный код посредством неопределённого вектора атаки.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:29543

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29543>

### CVE-2015-0308 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2015-0308](#)

Уязвимость

Риск: Высокий

ALTX ID  
63824

**Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленнику получить доступ к конфиденциальной информации (CVE-2015-0307)**

#### Описание

Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленнику получить доступ к конфиденциальной информации посредством неопределённого вектора атаки.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:29542

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29542>

### CVE-2015-0307 (CVE)

CVSS: Базовая оценка 8.5 (AV:N/AC:L/Au:N/C:P/I:N/A:C)

CWE: CWE-119

[CVE-2015-0307](#)

Уязвимость

Риск: Высокий

ALTX ID  
63825

**Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) (CVE-2015-0306)**

#### Описание

Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании (повреждение памяти) посредством неопределённого вектора атаки.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:29541

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29541>

### CVE-2015-0306 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2015-0306](#)

Уязвимость

Риск: Высокий

ALTX ID  
69496

**Неопределённая уязвимость в Oracle Java SE 6u91, 7u76, и 8u40 (CVE-2015-0458)**

#### Описание

Неопределённая уязвимость в Oracle Java SE 6u91, 7u76, и 8u40 позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки, связанных с развёртыванием.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

### Ссылки

oval:ru.altx-soft.win:def:38756

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38756>

### CVE-2015-0458 (CVE)

CVSS: Базовая оценка 7.6 (AV:N/AC:H/Au:N/C:C/I:C/A:C)

[CVE-2015-0458](#)

### Уязвимость

Риск: Высокий

ALTX ID  
72099

**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3086)**

### Описание

Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет злоумышленникам выполнить произвольный код. Уязвимость отлична от CVE-2015-3077 и CVE-2015-3084.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

### Ссылки

oval:ru.altx-soft.win:def:38993

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38993>

### CVE-2015-3086 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2015-3086](#)

### Уязвимость

Риск: Высокий

ALTX ID  
72097

**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3084)**

### Описание

Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет злоумышленникам выполнить произвольный код. Уязвимость отлична от CVE-2015-3077 и CVE-2015-3086.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

### Ссылки

oval:ru.altx-soft.win:def:38991

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38991>

### CVE-2015-3084 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2015-3084](#)

### Уязвимость

Риск: Высокий

ALTX ID  
72093

**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3080)**

### Описание

Уязвимость доступа к освобожденной памяти в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

### Ссылки

oval:ru.altx-soft.win:def:38987

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38987>

### CVE-2015-3080 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2015-3080](#)

### Уязвимость

Риск: Высокий

ALTX ID  
72100

**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3087)**

### Описание

Уязвимость целочисленного переполнение в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

### Ссылки

oval:ru.altx-soft.win:def:38994

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38994>

### CVE-2015-3087 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2015-3087](#)

### Уязвимость

Риск: Высокий

ALTX ID  
72103

**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3090)**

### Описание

Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2015-3078, CVE-2015-3089, и CVE-2015-3093.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

### Ссылки

oval:ru.altx-soft.win:def:38997

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38997>



### CVE-2015-3090 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2015-3090](#)

Уязвимость

Риск: Высокий

ALTX ID  
72102

**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3089)**

Описание

Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2015-3078, CVE-2015-3090, и CVE-2015-3093.

Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

Ссылки

oval:ru.altx-soft.win:def:38996

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38996>

### CVE-2015-3089 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2015-3089](#)

Уязвимость

Риск: Высокий

ALTX ID  
72101

**Уязвимость переполнения кучи в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3088)**

Описание

Уязвимость переполнения кучи в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

Ссылки

oval:ru.altx-soft.win:def:38995

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38995>

### CVE-2015-3088 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2015-3088](#)

Уязвимость

Риск: Высокий

ALTX ID  
72091

**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3078)**

Описание

Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством

неопределённых векторов атаки. Уязвимость отлична от CVE-2015-3089, CVE-2015-3090, и CVE-2015-3093.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

#### Ссылки

**oval:ru.altx-soft.win:def:38985**

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38985>

#### CVE-2015-3078 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2015-3078](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
69504

**Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0469)**

#### Описание

Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки, связанных с 2D.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

#### Ссылки

**oval:ru.altx-soft.win:def:38764**

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38764>

#### CVE-2015-0469 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2015-0469](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
69503

**Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0460)**

#### Описание

Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки, связанных с Hotspot.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

#### Ссылки

**oval:ru.altx-soft.win:def:38763**

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38763>

#### CVE-2015-0460 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

[CVE-2015-0460](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
69497**Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 позволяет (CVE-2015-0459)****Описание**

Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки, связанных с 2D. Уязвимость отлична от CVE-2015-0491.

**Исправление**

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

**Ссылки****oval:ru.altx-soft.win:def:38757**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38757>**CVE-2015-0459 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2015-0459](#)**Уязвимость**

Риск: Высокий

ALTX ID  
69514**Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0491)****Описание**

Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40, позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки, связанных с 2D. Уязвимость отлична от CVE-2015-0459.

**Исправление**

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

**Ссылки****oval:ru.altx-soft.win:def:38774**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38774>**CVE-2015-0491 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2015-0491](#)**Уязвимость**

Риск: Высокий

ALTX ID  
72090**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3077)****Описание**

Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет злоумышленникам выполнить произвольный код. Уязвимость отлична от CVE-2015-3084 и CVE-2015-3086.

**Исправление**

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

**Ссылки**

oval:ru.altx-soft.win:def:38984

<http://www.ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38984>

**CVE-2015-3077 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2015-3077](#)

<b>Уязвимость</b>	Риск: Высокий
<b>ALTX ID</b> 72047	<b>Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3093)</b>

**Описание**  
Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2015-3078, CVE-2015-3089, и CVE-2015-3090.

**Исправление**  
Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

**Ссылки**

oval:ru.altx-soft.win:def:38941

<http://www.ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38941>

**CVE-2015-3093 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2015-3093](#)

<b>Уязвимость</b>	Риск: Высокий
<b>ALTX ID</b> 69515	<b>Неопределённая уязвимость в Oracle Java SE 7u76 и 8u40 (CVE-2015-0492)</b>

**Описание**  
Неопределённая уязвимость в Oracle Java SE 7u76 и 8u40, позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2015-0484.

**Исправление**  
Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

**Ссылки**

oval:ru.altx-soft.win:def:38775

<http://www.ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38775>

**CVE-2015-0492 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

[CVE-2015-0492](#)

<b>Уязвимость</b>	Риск: Высокий
<b>ALTX ID</b> 56089	<b>Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player (CVE-2012-0763)</b>

**Описание**

Компонент Shockwave 3D Asset в Adobe Shockwave Player до версии 11.6.4.634 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29355

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29355>

#### CVE-2012-0763 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-0763](#)

Уязвимость

Риск: Высокий

ALTX ID  
56088

#### Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player (CVE-2012-0762)

#### Описание

Компонент Shockwave 3D Asset в Adobe Shockwave Player до версии 11.6.4.634 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29354

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29354>

#### CVE-2012-0762 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-0762](#)

Уязвимость

Риск: Высокий

ALTX ID  
56087

#### Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player (CVE-2012-0761)

#### Описание

Компонент Shockwave 3D Asset в Adobe Shockwave Player до версии 11.6.4.634 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29353

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29353>

#### CVE-2012-0761 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-0761](#)

Уязвимость

Риск: Высокий

ALTX ID  
56090

## Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player (CVE-2012-0764)

### Описание

Компонент Shockwave 3D Asset в Adobe Shockwave Player до версии 11.6.4.634 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:29356

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29356>

### CVE-2012-0764 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-0764](#)

### Уязвимость

Риск: Высокий

ALTX ID  
56093

## Повреждение памяти в Adobe Shockwave Player (CVE-2012-2030)

### Описание

Adobe Shockwave Player до версии 11.6.5.635 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:29359

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29359>

### CVE-2012-2030 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-2030](#)

### Уязвимость

Риск: Высокий

ALTX ID  
56092

## Повреждение памяти в Adobe Shockwave Player (CVE-2012-2029)

### Описание

Adobe Shockwave Player до версии 11.6.5.635 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:29358

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29358>

**CVE-2012-2029 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-2029](#)**Уязвимость**

Риск: Высокий

**ALT X ID**

56091

**Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player (CVE-2012-0766)****Описание**

Компонент Shockwave 3D Asset в Adobe Shockwave Player до версии 11.6.4.634 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29357**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29357>**CVE-2012-0766 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-0766](#)**Уязвимость**

Риск: Высокий

**ALT X ID**

56086

**Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player до версии 11.6.4.634 (CVE-2012-0760)****Описание**

Компонент Shockwave 3D Asset в Adobe Shockwave Player до версии 11.6.4.634 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29352**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29352>**CVE-2012-0760 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-0760](#)**Уязвимость**

Риск: Высокий

**ALT X ID**

56081

**Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2011-2447)****Описание**

Adobe Shockwave Player до версии 11.6.3.633 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29347

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29347>

#### CVE-2011-2447 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2447](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
56080

**Повреждение памяти в Adobe Shockwave Player, связанное с библиотекой DIRapi (CVE-2011-2448)**

#### Описание

Библиотека Dirapi в Adobe Shockwave Player до версии 11.6.3.633 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29346

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29346>

#### CVE-2011-2448 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2448](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
56079

**Многочисленные повреждения памяти в Adobe Shockwave Player (CVE-2011-2449)**

#### Описание

Модуль TextXtra в Adobe Shockwave Player до версии 11.6.3.633 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29345

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29345>

#### CVE-2011-2449 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2449](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
56082

**Повреждение памяти в Adobe Shockwave Player, связанное с библиотекой DIRapi (CVE-2011-2446)**



### Описание

Библиотека Dirapi в Adobe Shockwave Player до версии 11.6.3.633 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:29348**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29348>

### CVE-2011-2446 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-2446](#)

### Уязвимость

Риск: Высокий

ALTIX ID  
56085

**Повреждение памяти в Adobe Shockwave Player до версии 11.6.4.634 (CVE-2012-0759)**

### Описание

Adobe Shockwave Player до версии 11.6.4.634 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:29351**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29351>

### CVE-2012-0759 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-0759](#)

### Уязвимость

Риск: Высокий

ALTIX ID  
56084

**Переполнение кучи в Adobe Shockwave Player до версии 11.6.4.634 (CVE-2012-0758)**

### Описание

Переполнение кучи в Adobe Shockwave Player до версии 11.6.4.634 позволяет злоумышленникам выполнить произвольный код.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:29350**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29350>

### CVE-2012-0758 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-0758](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
56083**Повреждение памяти в Shockwave 3D Asset в Adobe Shockwave Player (CVE-2012-0757)****Описание**

Библиотека Dirapi в Adobe Shockwave Player до версии 11.6.3.633 позволяет удаленным злоумышленникам выполнить произвольный код или вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29349**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29349>**CVE-2012-0757 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-0757](#)**Уязвимость**

Риск: Высокий

ALTX ID  
56094**Повреждение памяти в Adobe Shockwave Player (CVE-2012-2031)****Описание**

Adobe Shockwave Player до версии 11.6.5.635 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29360**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29360>**CVE-2012-2031 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-2031](#)**Уязвимость**

Риск: Высокий

ALTX ID  
56105**Переполнение буфера в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2012-4173)****Описание**

Переполнение буфера в Adobe Shockwave Player до версии 11.6.7.638 позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29371**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29371>

### CVE-2012-4173 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-4173](#)

Уязвимость

Риск: Высокий

ALT X ID

56104

**Переполнение буфера в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2012-4174)**

Описание

Переполнение буфера в Adobe Shockwave Player до версии 11.6.7.638 позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.win:def:29370

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29370>

### CVE-2012-4174 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-4174](#)

Уязвимость

Риск: Высокий

ALT X ID

56103

**Переполнение буфера в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2012-4175)**

Описание

Переполнение буфера в Adobe Shockwave Player до версии 11.6.7.638 позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.win:def:29369

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29369>

### CVE-2012-4175 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-4175](#)

Уязвимость

Риск: Высокий

ALT X ID

56106

**Переполнение буфера в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2012-4172)**

Описание

Переполнение буфера в Adobe Shockwave Player до версии 11.6.7.638 позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29372

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29372>

#### CVE-2012-4172 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-4172](#)

#### Уязвимость

Риск: Высокий

#### ALTX ID

56111

### Переполнение буфера в Adobe Shockwave Player (CVE-2013-0636)

#### Описание

Переполнение буфера в Adobe Shockwave Player до версии 11.6.8.638 позволяет удалённым злоумышленникам выполнить произвольный код.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29377

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29377>

#### CVE-2013-0636 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2013-0636](#)

#### Уязвимость

Риск: Высокий

#### ALTX ID

56110

### Повреждение памяти в Adobe Shockwave Player (CVE-2013-0635)

#### Описание

Adobe Shockwave Player до версии 11.6.8.638 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:29376

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29376>

#### CVE-2013-0635 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2013-0635](#)

#### Уязвимость

Риск: Высокий

#### ALTX ID

56107

### Выход за границу массива в Adobe Shockwave Player (CVE-2012-4176)

### Описание

Ошибка индекса массива в Adobe Shockwave Player до версии 11.6.7.638 позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:29373**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29373>

### CVE-2012-4176 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2012-4176](#)

### Уязвимость

Риск: Высокий

ALTX ID  
56102

**Переполнение буфера в Adobe Shockwave Player до версии 11.6.7.638 посредством неопределённых векторов атаки (CVE-2012-5273)**

### Описание

Adobe Shockwave Player до версии 11.6.7.638 позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:29368**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29368>

### CVE-2012-5273 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-5273](#)

### Уязвимость

Риск: Высокий

ALTX ID  
56097

**Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (CVE-2012-2043)**

### Описание

Adobe Shockwave Player до версии 11.6.6.636 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:29363**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29363>

### CVE-2012-2043 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-2043](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
56096**Повреждение памяти в Adobe Shockwave Player (CVE-2012-2033)****Описание**

Adobe Shockwave Player до версии 11.6.5.635 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29362**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29362>**CVE-2012-2033 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-2033](#)**Уязвимость**

Риск: Высокий

ALTX ID  
56095**Повреждение памяти в Adobe Shockwave Player (CVE-2012-2032)****Описание**

Adobe Shockwave Player до версии 11.6.5.635 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29361**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29361>**CVE-2012-2032 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-2032](#)**Уязвимость**

Риск: Высокий

ALTX ID  
56098**Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (II) (CVE-2012-2044)****Описание**

Adobe Shockwave Player до версии 11.6.6.636 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29364**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29364>

**CVE-2012-2044 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-2044](#)**Уязвимость**

Риск: Высокий

**ALTX ID**

56101

**Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (V) (CVE-2012-2047)****Описание**

Adobe Shockwave Player до версии 11.6.6.636 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29367**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29367>**CVE-2012-2047 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-2047](#)**Уязвимость**

Риск: Высокий

**ALTX ID**

56100

**Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (IV) (CVE-2012-2046)****Описание**

Adobe Shockwave Player до версии 11.6.6.636 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:29366**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29366>**CVE-2012-2046 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-2046](#)**Уязвимость**

Риск: Высокий

**ALTX ID**

56099

**Повреждение памяти в Adobe Shockwave Player посредством неопределённых векторов атаки (III) (CVE-2012-2045)****Описание**

Adobe Shockwave Player до версии 11.6.6.636 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании.

**Исправление**

Необходимо установить актуальное обновление от производителя.

#### Ссылки

**oval:ru.altx-soft.win:def:29365**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29365>

#### CVE-2012-2045 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2012-2045](#)

Уязвимость

Риск: Высокий

ALTX ID  
23713

### Переполнение буфера в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1288)

#### Описание

Переполнение буфера в Adobe Shockwave Player до 11.5.7.609 позволяет удаленным злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

**oval:ru.altx-soft.win:def:22879**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22879>

#### CVE-2010-1288 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-1288](#)

Уязвимость

Риск: Высокий

ALTX ID  
23712

### Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1289)

#### Описание

Adobe Shockwave Player до 11.5.7.609 позволяет злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код посредством неопределённых векторов атак. Уязвимость отлична от CVE-2010-1284, CVE-2010-1286, CVE-2010-1287, CVE-2010-1290, и CVE-2010-1291.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

**oval:ru.altx-soft.win:def:22878**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22878>

#### CVE-2010-1289 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-1289](#)

Уязвимость

Риск: Высокий



ALTX ID  
23711

## Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1290)

### Описание

Adobe Shockwave Player до 11.5.7.609 позволяет злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код посредством неопределённых векторов атак. Уязвимость отлична от CVE-2010-1284, CVE-2010-1286, CVE-2010-1287, CVE-2010-1289, и CVE-2010-1291.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:22877

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22877>

### CVE-2010-1290 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-1290](#)

### Уязвимость

Риск: Высокий

ALTX ID  
23714

## Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1287)

### Описание

Adobe Shockwave Player до 11.5.7.609 позволяет злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код посредством неопределённых векторов атак. Уязвимость отлична от CVE-2010-1284, CVE-2010-1286, CVE-2010-1289, CVE-2010-1290, и CVE-2010-1291.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:22880

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22880>

### CVE-2010-1287 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-1287](#)

### Уязвимость

Риск: Высокий

ALTX ID  
23717

## Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1283)

### Описание

Adobe Shockwave Player до 11.5.7.609 не правильно обрабатывает 3D объекты в .dir (aka Director) файлах, что позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение кучи) через изменение поля в 0xFFFFFFFF49 записи.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:22883

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22883>

#### CVE-2010-1283 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-1283](#)

Уязвимость

Риск: Высокий

ALTX ID  
23716

**Множественные повреждения памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1284)**

#### Описание

Adobe Shockwave Player до 11.5.7.609 позволяет злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код посредством неопределённых векторов атак. Уязвимость отлична от CVE-2010-1286, CVE-2010-1287, CVE-2010-1289, CVE-2010-1290, и CVE-2010-1291.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22882

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22882>

#### CVE-2010-1284 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-1284](#)

Уязвимость

Риск: Высокий

ALTX ID  
23715

**Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1286)**

#### Описание

Adobe Shockwave Player до 11.5.7.609 позволяет злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код посредством неопределённых векторов атак. Уязвимость отлична от CVE-2010-1284, CVE-2010-1287, CVE-2010-1289, CVE-2010-1290, и CVE-2010-1291.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22881

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22881>

#### CVE-2010-1286 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-1286](#)

Уязвимость

Риск: Высокий

ALTX ID  
23218

**Переополнение кучи в TextXtra.x32 в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-2582)**

#### Описание

Неопределённая функция в TextXtra.x32 в Adobe Shockwave Player 11.5.9.615 и ниже ненадлежащим образом

перераспределяет буфер при обработке DEMX chunk в Director файле, что позволяет удалённым злоумышленникам вызвать а переполнение кучи и выполнить произвольный код.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22484

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22484>

#### CVE-2010-2582 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2582](#)

#### Уязвимость

Риск: Высокий

#### ALT X ID

23193

**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2863)**

#### Описание

Adobe Shockwave Player до 11.5.8.612 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) выполнить произвольный код посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22459

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22459>

#### CVE-2010-2863 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2863](#)

#### Уязвимость

Риск: Высокий

#### ALT X ID

23192

**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2864)**

#### Описание

IML32.dll в Adobe Shockwave Player до 11.5.8.612 ненадлежащим образом разбирает .dir файлы, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код через поврежденный файл, содержащий недопустимое значение.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22458

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22458>

#### CVE-2010-2864 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2864](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
23219**Уязвимость DoS в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-2581)****Описание**

dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) через Director файл, содержащий специально сформированный ram chunk с поврежденным размером или числом sub-chunk. Уязвимость отлична от CVE-2010-4084, CVE-2010-4085, CVE-2010-4086, и CVE-2010-4088.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:22485**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22485>**CVE-2010-2581 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2581](#)**Уязвимость**

Риск: Высокий

ALTX ID  
23710**Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1291)****Описание**

Adobe Shockwave Player до 11.5.7.609 позволяет злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код посредством неопределённых векторов атак. Уязвимость отлична от CVE-2010-1284, CVE-2010-1286, CVE-2010-1287, CVE-2010-1289, и CVE-2010-1290.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:22876**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22876>**CVE-2010-1291 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-1291](#)**Уязвимость**

Риск: Высокий

ALTX ID  
23709**Уязвимость в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1292)****Описание**

Реализация ram RIFF chunk парсера в Adobe Shockwave Player до 11.5.7.609 не проверяет определенное значение из файла до его использования в вычислениях указателя, что позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством специально сформированного .dir (aka Director) файла.

**Исправление**

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22875

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22875>

#### CVE-2010-1292 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2010-1292](#)

#### Уязвимость

Риск: Высокий

ALT X ID  
23646

**Неопределённая уязвимость в Spatial компоненте Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2012-3220)**

#### Описание

Неопределённая уязвимость в Spatial компоненте Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 позволяет удалённым авторизованным пользователям с Create Table привилегиями влиять на конфиденциальность, целостность, и доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22784

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22784>

#### CVE-2012-3220 (CVE)

CVSS: Базовая оценка 9 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

[CVE-2012-3220](#)

#### Уязвимость

Риск: Высокий

ALT X ID  
23719

**Уязвимость в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1281)**

#### Описание

iml32.dll в Adobe Shockwave Player до 11.5.7.609 does not validate a certain value from a file до using it in file-pointer calculations, что позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) через специально сформированный .dir (aka Director) файл.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22885

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22885>

#### CVE-2010-1281 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-1281](#)

#### Уязвимость

Риск: Высокий

ALT X ID  
64345

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0577)**

### Описание

Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 позволяет злоумышленникам выполнить произвольный код. Уязвимость отлична от CVE-2014-0584, CVE-2014-0585, CVE-2014-0586, и CVE-2014-0590.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

### Ссылки

oval:ru.altx-soft.win:def:24643

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24643>

### CVE-2014-0577 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-94

[CVE-2014-0577](#)

### apsb14-24 (Adobe)

[apsb14-24](#)

### Уязвимость

Риск: Высокий

ALTX ID  
64344

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0576)**

### Описание

Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0581, CVE-2014-8440, и CVE-2014-8441.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

### Ссылки

oval:ru.altx-soft.win:def:24642

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24642>

### CVE-2014-0576 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2014-0576](#)

### apsb14-24 (Adobe)

[apsb14-24](#)

### Уязвимость

Риск: Высокий

ALTX ID  
64343

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0574)**

### Описание

Уязвимость двойного освобождения в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356, позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

### Ссылки

oval:ru.altx-soft.win:def:24641

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24641>

**CVE-2014-0574 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-94

[CVE-2014-0574](#)

**apsb14-24 (Adobe)**

[apsb14-24](#)

Уязвимость

Риск: Высокий

ALTX ID  
64346

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0581)**

**Описание**

Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0576, CVE-2014-8440, и CVE-2014-8441.

**Исправление**

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

**Ссылки**

**oval:ru.altx-soft.win:def:24644**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24644>

**CVE-2014-0581 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2014-0581](#)

**apsb14-24 (Adobe)**

[apsb14-24](#)

Уязвимость

Риск: Высокий

ALTX ID  
64349

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0583)**

**Описание**

Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356, позволяет злоумышленникам выполнить произвольный код. Уязвимость отлична от CVE-2014-0577, CVE-2014-0585, CVE-2014-0586, и CVE-2014-0590.

**Исправление**

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

**Ссылки**

**oval:ru.altx-soft.win:def:24647**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24647>

**CVE-2014-0584 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-94

[CVE-2014-0584](#)

**apsb14-24 (Adobe)**

[apsb14-24](#)

<b>Уязвимость</b>	Риск: Высокий
ALTX ID 64348	<b>Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0583)</b>
<b>Описание</b>	Переполнение кучи в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356.
<b>Исправление</b>	Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <a href="http://get.adobe.com/ru/air/">http://get.adobe.com/ru/air/</a> , <a href="http://get.adobe.com/ru/flashplayer/">http://get.adobe.com/ru/flashplayer/</a> .
<b>Ссылки</b>	<p><b>oval:ru.altx-soft.win:def:24646</b>  <a href="http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24646">http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24646</a></p> <p><b>CVE-2014-0583 (CVE)</b>  CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)  CWE: CWE-119  <a href="#">CVE-2014-0583</a></p> <p><b>aprb14-24 (Adobe)</b>  <a href="#">aprb14-24</a></p>

<b>Уязвимость</b>	Риск: Высокий
ALTX ID 64347	<b>Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0582)</b>
<b>Описание</b>	Переполнение кучи в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356, позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0589.
<b>Исправление</b>	Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <a href="http://get.adobe.com/ru/air/">http://get.adobe.com/ru/air/</a> , <a href="http://get.adobe.com/ru/flashplayer/">http://get.adobe.com/ru/flashplayer/</a> .
<b>Ссылки</b>	<p><b>oval:ru.altx-soft.win:def:24645</b>  <a href="http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24645">http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24645</a></p> <p><b>CVE-2014-0582 (CVE)</b>  CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)  CWE: CWE-119  <a href="#">CVE-2014-0582</a></p> <p><b>aprb14-24 (Adobe)</b>  <a href="#">aprb14-24</a></p>

<b>Уязвимость</b>	Риск: Высокий
ALTX ID 23767	<b>Повреждение памяти в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-0986)</b>
<b>Описание</b>	Adobe Shockwave Player до 11.5.7.609 не правильно обрабатывает записи asset, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код через специально сформированный Shockwave файл.



### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:22933

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22933>

### CVE-2010-0986 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-0986](#)

### Уязвимость

Риск: Высокий

### ALT X ID

23766

### Переполнение кучи в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-0987)

### Описание

Переполнение кучи в Adobe Shockwave Player до 11.5.7.609 позволяет удалённым злоумышленникам выполнить произвольный код через специально сформированные встроенные шрифты в Shockwave файле.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:22932

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22932>

### CVE-2010-0987 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-0987](#)

### Уязвимость

Риск: Высокий

### ALT X ID

23720

### Уязвимость в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1280)

### Описание

Adobe Shockwave Player до 11.5.7.609 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) через специально сформированный .dir (aka Director) файл.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:22886

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22886>

### CVE-2010-1280 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-1280](#)

### Уязвимость

Риск: Высокий

ALTX ID 58121	<b>Adobe Flash Player до 13.0.0.250 и 14.x и 15.x до 15.0.0.189, Adobe AIR до 15.0.0.293 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) (CVE-2014-0558)</b>
------------------	---

#### Описание

Adobe Flash Player до 13.0.0.250 и 14.x и 15.x до 15.0.0.189, Adobe AIR до 15.0.0.293 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0564.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

**oval:ru.altx-soft.win:def:24187**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24187>

**CVE-2014-0558 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-94

[CVE-2014-0558](#)

**aprb14-22 (Adobe)**

[aprb14-22](#)

#### Уязвимость

Риск: Высокий

ALTX ID 64342	<b>Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0573)</b>
------------------	---

#### Описание

Уязвимость доступа к освобожденной памяти в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0588 и CVE-2014-8438.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

**oval:ru.altx-soft.win:def:24640**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24640>

**CVE-2014-0573 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2014-0573](#)

**aprb14-24 (Adobe)**

[aprb14-24](#)

#### Уязвимость

Риск: Высокий

ALTX ID 58123	<b>Adobe Flash Player до 13.0.0.250 и 14.x и 15.x до 15.0.0.189, Adobe AIR до 15.0.0.293 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) (CVE-2014-0569)</b>
------------------	---

#### Описание

Целочисленное переполнение в Adobe Flash Player до 13.0.0.250 и 14.x и 15.x до 15.0.0.189, Adobe AIR до 15.0.0.293 позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:24189

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24189>

**CVE-2014-0569 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2014-0569](#)

apsb14-22 (Adobe)

[apsb14-22](#)

#### Уязвимость

Риск: Высокий

#### ALTX ID

58122

**Adobe Flash Player до 13.0.0.250 и 14.x и 15.x до 15.0.0.189, Adobe AIR до 15.0.0.293 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) (CVE-2014-0564)**

#### Описание

Adobe Flash Player до 13.0.0.250 и 14.x и 15.x до 15.0.0.189, Adobe AIR до 15.0.0.293 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0558.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:24188

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24188>

**CVE-2014-0564 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2014-0564](#)

apsb14-22 (Adobe)

[apsb14-22](#)

#### Уязвимость

Риск: Высокий

#### ALTX ID

23190

**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2866)**

#### Описание

Ошибка знакового в DIRAPI модуле Adobe Shockwave Player до 11.5.8.612 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код через значение count, связанное с недокументированной структурой и tSAC chunk в Director видеофайле.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22456

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22456>

**CVE-2010-2866 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2010-2866](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
22969**Повреждение памяти в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-4085)****Описание**

dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2010-2581, CVE-2010-4084, CVE-2010-4086, и CVE-2010-4088.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:22229**<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22229>**CVE-2010-4085 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4085](#)**Уязвимость**

Риск: Высокий

ALTX ID  
22968**Уязвимость DoS в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-4086)****Описание**

dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) через специально сформированный .dir файл с повреждённым размером элемента. Уязвимость отлична от CVE-2010-2581, CVE-2010-2880, CVE-2010-4084, CVE-2010-4085, и CVE-2010-4088.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:22228**<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22228>**CVE-2010-4086 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4086](#)**Уязвимость**

Риск: Высокий

ALTX ID  
22967**Уязвимость DoS в IML32.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-4087)****Описание**

IML32.dll в Adobe Shockwave Player 11.5.9.615 и ниже позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) через .dir файл со специально сформированной mmap записью, содержащую повреждённую длину VSWV записи. Уязвимость отлична от CVE-2010-4089.

**Исправление**

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22227

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22227>

#### CVE-2010-4087 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4087](#)

Уязвимость

Риск: Высокий

ALT X ID  
22970

**Уязвимость DoS в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-4084)**

#### Описание

dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2010-2581, CVE-2010-4085, CVE-2010-4086, и CVE-2010-4088.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22230

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22230>

#### CVE-2010-4084 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4084](#)

Уязвимость

Риск: Высокий

ALT X ID  
23174

**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2882)**

#### Описание

DIRAPI.dll в Adobe Shockwave Player до 11.5.8.612 ненадлежащим образом разбирает .dir файлы, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код через поврежденный файл, содержащий недопустимое значение.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22440

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22440>

#### CVE-2010-2882 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2882](#)

Уязвимость

Риск: Высокий

ALT X ID  
23049

**Повреждение памяти в Director модуле (dirapi.dll) Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-3653)**

### Описание

Модуль Director (dirapi.dll) в Adobe Shockwave Player 11.5.9.615 и ниже позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) через Director видео со специально сформированным gcsL chunk, содержит поле, значение которого используется как смещение указателя.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:22311

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22311>

**CVE-2010-3653 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-3653](#)

### Уязвимость

Риск: Высокий

ALTX ID  
23048

**Переполнение стека в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-3655)**

### Описание

Переполнение стека в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:22310

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22310>

**CVE-2010-3655 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-3655](#)

### Уязвимость

Риск: Высокий

ALTX ID  
21340

**Уязвимость целочисленного переполнения в Adobe Shockwave Player (CVE-2009-4003)**

### Описание

Множество целочисленных переполнений в Adobe Shockwave Player до 11.5.6.606 позволяют удалённым злоумышленникам выполнить произвольный код через неопределённый тип блока в файле Shockwave, что приводит к переполнению буфера или повреждению кучи.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:21374

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:21374>

### CVE-2009-4003 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2009-4003](#)

Уязвимость

Риск: Высокий

ALTX ID

19549

**Уязвимость в Active Directory, связанная с переполнением буфера (CVE-2011-3406)**

Описание

В Active Directory существует уязвимость, делающая возможным удаленное выполнение кода. Для использования этой уязвимости злоумышленнику потребуется получить учетные данные для входа в домен Active Directory. Затем он может запустить специальное приложение, способное воспользоваться уязвимостью, и таким образом установить контроль над уязвимой системой. После этого злоумышленник сможет устанавливать программы, просматривать, изменять и уничтожать данные или создавать новые учетные записи с неограниченными правами.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.win:def:12392

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:12392>

### CVE-2011-3406 (CVE)

CVSS: Базовая оценка 9 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2011-3406](#)

### MS11-095 (Microsoft)

[MS11-095](#)

Уязвимость

Риск: Высокий

ALTX ID

19545

**Уязвимость, связанная с обходом проверки подлинности LDAPS (CVE-2011-2014)**

Описание

В службе Active Directory существует уязвимость, делающая возможным несанкционированное получение прав, если данная служба настроена на использование LDAP через SSL (LDAPS). Злоумышленник может воспользоваться этой уязвимостью, используя ранее отозванный сертификат для прохождения проверки подлинности в домене Active Directory и получения доступа к сетевым ресурсам или выполнения кода с правами конкретного авторизованного пользователя, с которым связан данный сертификат.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.win:def:12372

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:12372>

### CVE-2011-2014 (CVE)

CVSS: Базовая оценка 9 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

CWE: CWE-287

[CVE-2011-2014](#)

### MS11-086 (Microsoft)

[MS11-086](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
22963**Уязвимость доступа к освобожденной памяти в Adobe Shockwave Player 11.5.9.620 и ниже (CVE-2010-4092)****Описание**

Уязвимость доступа к освобожденной памяти в Adobe Shockwave Player 11.5.9.620 и ниже позволяет при содействии пользователя удалённым злоумышленникам выполнить произвольный код через специально сформированный web сайт.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:22223**<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22223>**CVE-2010-4092 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-399

[CVE-2010-4092](#)**Уязвимость**

Риск: Высокий

ALTX ID  
22966**Уязвимость в dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-4088)****Описание**

dirapi.dll в Adobe Shockwave Player 11.5.9.615 и ниже позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) через .dir файл, содержащий дублированные ссылки на часть KEY\* chunk. Уязвимость отлична от CVE-2010-2581, CVE-2010-4084, CVE-2010-4085, и CVE-2010-4086.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:22226**<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22226>**CVE-2010-4088 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4088](#)**Уязвимость**

Риск: Высокий

ALTX ID  
22965**Уязвимость в IML32.dll в Adobe Shockwave Player 11.5.9.615 и ниже (CVE-2010-4089)****Описание**

IML32.dll в Adobe Shockwave Player 11.5.9.615 и ниже позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) через .dir файл, содержащий дублированные записи LCSM в mтар записи. Уязвимость отлична от CVE-2010-4087.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**



oval:ru.altx-soft.win:def:22225

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22225>

**CVE-2010-4089 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4089](#)

Уязвимость

Риск: Высокий

ALTX ID  
22964

**Уязвимость в Adobe Shockwave Player 11.5.9.615 и ниже позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки (CVE-2010-4090)**

**Описание**

Adobe Shockwave Player 11.5.9.615 и ниже позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:22224

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22224>

**CVE-2010-4090 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-4090](#)

Уязвимость

Риск: Высокий

ALTX ID  
23175

**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2881)**

**Описание**

IML32.dll в Adobe Shockwave Player до 11.5.8.612 ненадлежащим образом разбирает .dir файлы, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код через поврежденный файл, содержащий недопустимое значение.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:22441

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22441>

**CVE-2010-2881 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2881](#)

Уязвимость

Риск: Высокий

ALTX ID  
23185

**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2871)**

**Описание**

Целочисленное переполнение в 3D object функциональности Adobe Shockwave Player до 11.5.8.612 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение кучи) и выполнить произвольный код через специально сформированный размер значения в 0xFFFFFFFF RIFF записи в Director видеофайле.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22451

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22451>

#### CVE-2010-2871 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2010-2871](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
23184

**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2872)**

#### Описание

Adobe Shockwave Player до 11.5.8.612 ненадлежащим образом проверяет смещение значения в ram1 RIFF chunk в Director видеофайле, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код через специально сформированный видеофайл.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22450

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22450>

#### CVE-2010-2872 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2010-2872](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
23183

**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2873)**

#### Описание

Adobe Shockwave Player до 11.5.8.612 ненадлежащим образом проверяет смещение значения в rcsL RIFF chunks .DIR и .DCR Director видеофайлах, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение кучи) и выполнить произвольный код через специально сформированный видеофайл.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22449

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22449>

#### CVE-2010-2873 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2010-2873](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
23186**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2870)****Описание**

DIRAPIX.dll в Adobe Shockwave Player до 11.5.8.612 ненадлежащим образом проверяет определенный chunk размер mmap chunk в Director видеофайле, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение кучи) и выполнить произвольный код через специально сформированный видеофайл.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:22452**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22452>**CVE-2010-2870 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2870](#)**Уязвимость**

Риск: Высокий

ALTX ID  
23189**Уязвимость смещения указателя в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2867)****Описание**

DIRAPIX.dll в Adobe Shockwave Player до 11.5.8.612 не правильно обрабатывает определенные возвращаемые значения, связанные с rcsL chunk в Director видеофайле, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение кучи) и выполнить произвольный код через специально сформированный видеофайл.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:22455**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22455>**CVE-2010-2867 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2867](#)**Уязвимость**

Риск: Высокий

ALTX ID  
23188**Множественные уязвимости в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2868)****Описание**

IML32.dll в Adobe Shockwave Player до 11.5.8.612 ненадлежащим образом разбирает .dir файлы, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) выполнить произвольный код через поврежденный файл, содержащий недопустимое значение.

**Исправление**

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22454

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22454>

#### CVE-2010-2868 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2868](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
23187

**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2869)**

#### Описание

IML32.dll в Adobe Shockwave Player до 11.5.8.612 ненадлежащим образом разбирает .dir файлы, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код через поврежденный файл, содержащий недопустимое значение.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22453

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22453>

#### CVE-2010-2869 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2869](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
23178

**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2878)**

#### Описание

DIRAPIX.dll в Adobe Shockwave Player до 11.5.8.612 ненадлежащим образом проверяет значение, связанное с буфером поиска в Director видеофайле, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение кучи) и выполнить произвольный код через специально сформированный видеофайл.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22444

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22444>

#### CVE-2010-2878 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2010-2878](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
23177

**Уязвимость целочисленного переполнения в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2879)**

## Описание

Множественные целочисленные переполнения в allocator в TextXtra.x32 модуле Adobe Shockwave Player до 11.5.8.612 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение кучи) и выполнить произвольный код через специально сформированный элемент count или size значение в файле.

## Исправление

Необходимо установить актуальное обновление от производителя.

## Ссылки

oval:ru.altx-soft.win:def:22443

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22443>

## CVE-2010-2879 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2010-2879](#)

## Уязвимость

Риск: Высокий

ALTX ID  
23176

**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2880)**

## Описание

DIRAPI.dll в Adobe Shockwave Player до 11.5.8.612 ненадлежащим образом разбирает .dir файлы, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код через поврежденный файл, содержащий недопустимое значение.

## Исправление

Необходимо установить актуальное обновление от производителя.

## Ссылки

oval:ru.altx-soft.win:def:22442

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22442>

## CVE-2010-2880 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-2880](#)

## Уязвимость

Риск: Высокий

ALTX ID  
23179

**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2877)**

## Описание

Adobe Shockwave Player до 11.5.8.612 ненадлежащим образом проверяет count значение в Director видеофайле, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение кучи) и выполнить произвольный код через специально сформированный видеофайл, связано с IML32X.dll и DIRAPIX.dll.

## Исправление

Необходимо установить актуальное обновление от производителя.

## Ссылки

oval:ru.altx-soft.win:def:22445

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22445>

**CVE-2010-2877 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2010-2877](#)**Уязвимость**

Риск: Высокий

ALTX ID  
23182**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2874)****Описание**

Неопределенная уязвимость в Adobe Shockwave Player до 11.5.8.612 позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки, вызывающих повреждение памяти.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:22448**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22448>**CVE-2010-2874 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-399

[CVE-2010-2874](#)**Уязвимость**

Риск: Высокий

ALTX ID  
23181**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2875)****Описание**

Ошибка знакового в Adobe Shockwave Player до 11.5.8.612 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код через длину значения, связанную с tSAC chunk в Director видеофайле.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:22447**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22447>**CVE-2010-2875 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2010-2875](#)**Уязвимость**

Риск: Высокий

ALTX ID  
23180**Уязвимость повреждения памяти в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2876)****Описание**

Adobe Shockwave Player до 11.5.8.612 ненадлежащим образом проверяет значения, связанные с расчетом размера буфера для 0xFFFFFFFF8 записи в .dir или .dcr Director видеофайле, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение кучи) и выполнить произвольный код через специально сформированный

видеофайл.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22446

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22446>

#### CVE-2010-2876 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-20

[CVE-2010-2876](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
64350

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0585)**

#### Описание

Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356, позволяет злоумышленникам выполнить произвольный код. Уязвимость отлична от CVE-2014-0577, CVE-2014-0584, CVE-2014-0586, и CVE-2014-0590.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:24648

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24648>

#### CVE-2014-0585 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-94

[CVE-2014-0585](#)

#### aprb14-24 (Adobe)

[aprb14-24](#)

#### Уязвимость

Риск: Высокий

ALTX ID  
31223

**Уязвимость в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-0127)**

#### Описание

Ошибка в Adobe Shockwave Player до 11.5.7.609 позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) через специально сформированный FFFFFFF45h Shockwave 3D блок в Shockwave файле.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:27706

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:27706>

#### CVE-2010-0127 (CVE)

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2010-0127](#)

**Уязвимость**

Риск: Высокий

ALTX ID  
31222**Ошибка знаковости в dirapi.dll в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-0128)****Описание**

Ошибка знаковости в dirapi.dll в Adobe Shockwave Player до 11.5.7.609 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код через специально сформированный .dig файл.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:27705**<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:27705>**CVE-2010-0128 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2010-0128](#)**Уязвимость**

Риск: Высокий

ALTX ID  
31221**Множественные целочисленные переполнения в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-0129)****Описание**

Множественные целочисленные переполнения в Adobe Shockwave Player до 11.5.7.609 позволяют удалённым злоумышленникам вызвать отказ в обслуживании (повреждение памяти) и выполнить произвольный код через специально сформированный .dig файл, вызывающий ошибку индексации массива.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:27704**<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:27704>**CVE-2010-0129 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2010-0129](#)**Уязвимость**

Риск: Высокий

ALTX ID  
31255**Уязвимость в Adobe Shockwave Player до 11.5.2.602 (CVE-2009-3465)****Описание**

Adobe Shockwave Player до 11.5.2.602 позволяет удалённым злоумышленникам выполнить произвольный код через специально сформированный Shockwave контент на веб-сайте.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**



oval:ru.altx-soft.win:def:27744

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:27744>

**CVE-2009-3465 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-94

[CVE-2009-3465](#)

<b>Уязвимость</b>	Риск: Высокий
<b>ALTX ID</b> 31254	<b>Уязвимость в Adobe Shockwave Player до 11.5.2.602 (CVE-2009-3466)</b>

**Описание**

Adobe Shockwave Player до 11.5.2.602 позволяет удалённым злоумышленникам выполнить произвольный код через специально сформированную веб-страницу, вызывающую повреждение памяти.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:27743

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:27743>

**CVE-2009-3466 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-399

[CVE-2009-3466](#)

<b>Уязвимость</b>	Риск: Высокий
<b>ALTX ID</b> 31248	<b>Переполнение кучи в Adobe Shockwave Player до 11.5.6.606 (CVE-2009-4002)</b>

**Описание**

Переполнение кучи в Adobe Shockwave Player до 11.5.6.606 позволяет удалённым злоумышленникам выполнить произвольный код через специально сформированную 3D модель в Shockwave файле.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:27734

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:27734>

**CVE-2009-4002 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2009-4002](#)

<b>Уязвимость</b>	Риск: Высокий
<b>ALTX ID</b> 64276	<b>Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-2253)</b>

**Описание**

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7,

11.2.0.1 и 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность, целостность и доступность, связано с SYSDBA.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25774

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25774>

#### CVE-2011-2253 (CVE)

CVSS: Базовая оценка 7.1 (AV:N/AC:H/Au:S/C:C/I:C/A:C)

[CVE-2011-2253](#)

Уязвимость

Риск: Высокий

ALTX ID

64304

**Уязвимость в TNS Listener в Oracle Database 11g 11.1.0.7, 11.2.0.2 и 11.2.0.3 и 10g 10.2.0.3, 10.2.0.4 и 10.2.0.5 (CVE-2012-1675)**

#### Описание

Уязвимость в TNS Listener в Oracle Database 11g 11.1.0.7, 11.2.0.2 и 11.2.0.3 и 10g 10.2.0.3, 10.2.0.4 и 10.2.0.5 позволяет удалённым злоумышленникам выполнить произвольные команды базы данных, выполняя удаленную регистрацию базы данных (1) и (2) instance, которое уже существует, для проведения man-in-the-middle (MITM) атаки и hijack подключений к базе данных.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25802

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25802>

#### CVE-2012-1675 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CWE: CWE-264

[CVE-2012-1675](#)

Уязвимость

Риск: Высокий

ALTX ID

64287

**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.2.0.2 (CVE-2012-0519)**

#### Описание

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25785

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25785>

#### CVE-2012-0519 (CVE)

CVSS: Базовая оценка 7.1 (AV:N/AC:H/Au:S/C:C/I:C/A:C)

[CVE-2012-0519](#)

Уязвимость

Риск: Высокий

ALTIX ID  
64270

**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-2239)**

#### Описание

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность, целостность и доступность, связано с XMLSEQ\_IMP\_T.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25768

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25768>

**CVE-2011-2239 (CVE)**

CVSS: Базовая оценка 7.1 (AV:N/AC:H/Au:S/C:C/I:C/A:C)

[CVE-2011-2239](#)

Уязвимость

Риск: Высокий

ALTIX ID  
31220

**Целочисленное переполнение в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-0130)**

#### Описание

Целочисленное переполнение в Adobe Shockwave Player до 11.5.7.609 позволяет удалённым злоумышленникам выполнить произвольный код через специально сформированный .dir файл.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:27703

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:27703>

**CVE-2010-0130 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-189

[CVE-2010-0130](#)

Уязвимость

Риск: Высокий

ALTIX ID  
64294

**Неопределённая уязвимость в Oracle Spatial компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-0552)**

#### Описание

Неопределённая уязвимость в Oracle Spatial компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25792

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25792>

**CVE-2012-0552 (CVE)**

CVSS: Базовая оценка 9 (AV:N/AC:L/Au:S/C:C/I:C/A:C)

[CVE-2012-0552](#)**Уязвимость**

Риск: Высокий

ALTX ID  
64359**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-8442)****Описание**

Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356.

**Исправление**Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.**Ссылки**

oval:ru.altx-soft.win:def:24657

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24657>**CVE-2014-8442 (CVE)**

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CWE: CWE-264

[CVE-2014-8442](#)**apsb14-24 (Adobe)**[apsb14-24](#)**Уязвимость**

Риск: Высокий

ALTX ID  
64353**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0589)****Описание**

Переполнение кучи в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356, позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0582.

**Исправление**Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.**Ссылки**

oval:ru.altx-soft.win:def:24651

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24651>**CVE-2014-0589 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2014-0589](#)**apsb14-24 (Adobe)**[apsb14-24](#)**Уязвимость**

Риск: Высокий

ALTX ID  
31257**Уязвимость в Adobe Shockwave Player до 11.5.2.602 (CVE-2009-3463)**

### Описание

Ошибка индексации массива в Adobe Shockwave Player до 11.5.2.602 позволяет удалённым злоумышленникам выполнить произвольный код через специально сформированный Shockwave контент на веб-сайте.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

**oval:ru.altx-soft.win:def:27746**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:27746>

**CVE-2009-3463 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-119

[CVE-2009-3463](#)

### Уязвимость

Риск: Высокий

ALT X ID  
64358

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-8441)**

### Описание

Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356, позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0576, CVE-2014-0581, и CVE-2014-8440.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

### Ссылки

**oval:ru.altx-soft.win:def:24656**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24656>

**CVE-2014-8441 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2014-8441](#)

**aprb14-24 (Adobe)**

[aprb14-24](#)

### Уязвимость

Риск: Высокий

ALT X ID  
64354

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0590)**

### Описание

Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356, позволяет злоумышленникам выполнить произвольный код, используя an unspecified "type confusion. Уязвимость отлична от CVE-2014-0577, CVE-2014-0584, CVE-2014-0585, и CVE-2014-0586.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

### Ссылки

**oval:ru.altx-soft.win:def:24652**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24652>

### CVE-2014-0590 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2014-0590](#)

apsb14-24 (Adobe)

[apsb14-24](#)

Уязвимость

Риск: Высокий

ALTX ID  
64356

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-8438)**

#### Описание

Уязвимость доступа к освобожденной памяти в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356, позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0573 и CVE-2014-0588.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:24654

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24654>

### CVE-2014-8438 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2014-8438](#)

apsb14-24 (Adobe)

[apsb14-24](#)

Уязвимость

Риск: Высокий

ALTX ID  
64357

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-8440)**

#### Описание

Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356, позволяет удалённым злоумышленникам выполнить произвольный код и вызвать отказ в обслуживании (повреждение памяти) посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0576, CVE-2014-0581, и CVE-2014-8441.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:24655

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24655>

### CVE-2014-8440 (CVE)

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2014-8440](#)

apsb14-24 (Adobe)

[apsb14-24](#)

Уязвимость

Риск: Высокий

ALTX ID

31256

**Уязвимость в Adobe Shockwave Player до 11.5.2.602 (CVE-2009-3464)**

#### Описание

Adobe Shockwave Player до 11.5.2.602 позволяет удалённым злоумышленникам выполнить произвольный код через специально сформированный Shockwave контент на веб-сайте.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

**oval:ru.altx-soft.win:def:27745**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:27745>

**CVE-2009-3464 (CVE)**

CVSS: Базовая оценка 9.3 (AV:N/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-94

[CVE-2009-3464](#)

**Уязвимость**

Риск: Высокий

ALTX ID

64352

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0588)**

#### Описание

Уязвимость доступа к освобожденной памяти в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356, позволяет удалённым злоумышленникам выполнить произвольный код посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2014-0573 и CVE-2014-8438.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

**oval:ru.altx-soft.win:def:24650**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24650>

**CVE-2014-0588 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

[CVE-2014-0588](#)

**aprb14-24 (Adobe)**

[aprb14-24](#)

**Уязвимость**

Риск: Высокий

ALTX ID

64351

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-0586)**

#### Описание

Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356, позволяет злоумышленникам выполнить произвольный код. Уязвимость отлична от CVE-2014-0577, CVE-2014-0584, CVE-2014-0585, и CVE-2014-0590.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

oval:ru.altx-soft.win:def:24649

<http://www.ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24649>

**CVE-2014-0586 (CVE)**

CVSS: Базовая оценка 10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CWE: CWE-94

[CVE-2014-0586](#)

**apsb14-24 (Adobe)**

[apsb14-24](#)

Уязвимость

Риск: Средний

ALTX ID  
66679

**Уязвимость в Wireshark 1.10.x до 1.10.13 и 1.12.x до 1.12.4 (CVE-2015-2189)**

**Описание**

Ошибка off-by-one в функции pcapng\_read в wiretap/pcapng.c в pcapng файл-парсере в Wireshark 1.10.x до 1.10.13 и 1.12.x до 1.12.4, позволяет удалённым злоумышленникам вызвать отказ в обслуживании (чтение за пределами выделенной памяти и падение приложения).

**Исправление**

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

**Ссылки**

oval:ru.altx-soft.win:def:38361

<http://www.ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38361>

**CVE-2015-2189 (CVE)**

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-189

[CVE-2015-2189](#)

Уязвимость

Риск: Средний

ALTX ID  
66677

**Уязвимость в Wireshark 1.12.x до 1.12.4 (CVE-2015-2187)**

**Описание**

Уязвимость в функции dissect\_atn\_cpdlc\_heur в asn1/atn-cpdlc/packet-atn-cpdlc-template.c в ATN-CPDLC диссекторе Wireshark 1.12.x до 1.12.4, позволяет удалённым злоумышленникам вызвать отказ в обслуживании (повреждение стека памяти и падение приложения) через специально сформированный пакет.

**Исправление**

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

**Ссылки**

oval:ru.altx-soft.win:def:38359

<http://www.ovaldb.ru/altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38359>

**CVE-2015-2187 (CVE)**

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-20

[CVE-2015-2187](#)

Уязвимость

Риск: Средний



ALTX ID

65605

**Незаполнение буфера в Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 (CVE-2015-0564)**

#### Описание

Незаполнение буфера в функции `ssl_decrypt_record` в `epan/dissectors/packet-ssl-utils.c` в Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (падение приложения) через специально сформированный пакет.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

#### Ссылки

**oval:ru.altx-soft.win:def:38047**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38047>

**CVE-2015-0564 (CVE)**

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-119

[CVE-2015-0564](#)

Уязвимость

Риск: Средний

ALTX ID

66678

**Уязвимость в Wireshark 1.10.x до 1.10.13 и 1.12.x до 1.12.4 (CVE-2015-2188)**

#### Описание

Уязвимость в `epan/dissectors/packet-wcp.c` в WCP диссекторе Wireshark 1.10.x до 1.10.13 и 1.12.x до 1.12.4 не должным образом инициализирует информацию, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (чтение за пределами выделенной памяти и падение приложения).

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

#### Ссылки

**oval:ru.altx-soft.win:def:38360**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38360>

**CVE-2015-2188 (CVE)**

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-19

[CVE-2015-2188](#)

Уязвимость

Риск: Средний

ALTX ID

66681

**Уязвимость в Wireshark 1.10.x до 1.10.13 и 1.12.x до 1.12.4 (CVE-2015-2191)**

#### Описание

Целочисленное переполнение в функции `dissect_tnef` в `epan/dissectors/packet-tnef.c` в TNEF диссекторе Wireshark 1.10.x до 1.10.13 и 1.12.x до 1.12.4, позволяет удалённым злоумышленникам вызвать отказ в обслуживании (бесконечный цикл).

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

#### Ссылки

oval:ru.altx-soft.win:def:38363

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38363>

**CVE-2015-2191 (CVE)**

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-189

[CVE-2015-2191](#)

Уязвимость

Риск: Средний

ALTX ID

66680

**Уязвимость в Wireshark 1.12.x до 1.12.4 (CVE-2015-2190)**

**Описание**

Уязвимость в epan/proto.c в Wireshark 1.12.x до 1.12.4 не правильно обрабатывает целочисленные типы данных больше чем 32 бита, что позволяет удалённым злоумышленникам вызвать отказ в обслуживании (сбой и завершение приложения).

**Исправление**

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

**Ссылки**

oval:ru.altx-soft.win:def:38362

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38362>

**CVE-2015-2190 (CVE)**

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-19

[CVE-2015-2190](#)

Уязвимость

Риск: Средний

ALTX ID

65596

**Множественные целочисленные переполнения в AMQP диссекторе Wireshark 1.10.x до 1.10.11 и 1.12.x до 1.12.2 (CVE-2014-8711)**

**Описание**

Множественные целочисленные переполнения в epan/dissectors/packet-amqp.c в AMQP диссекторе Wireshark 1.10.x до 1.10.11 и 1.12.x до 1.12.2 позволяют удалённым злоумышленникам вызвать отказ в обслуживании (падение приложения) через специально сформированный amqp\_0\_10 PDU пакет.

**Исправление**

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

**Ссылки**

oval:ru.altx-soft.win:def:38038

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38038>

**CVE-2014-8711 (CVE)**

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-189

[CVE-2014-8711](#)

Уязвимость

Риск: Средний

ALTX ID

66682

**Уязвимость в Wireshark 1.12.x до 1.12.4 (CVE-2015-2192)**

### Описание

Целочисленное переполнение в функции `dissect_osd2_cdb_continuation` в `epan/dissectors/packet-scsi-osd.c` в SCSI OSD диссекторе Wireshark 1.12.x до 1.12.4 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (бесконечный цикл).

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

### Ссылки

**oval:ru.altx-soft.win:def:38364**

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38364>

### CVE-2015-2192 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-189

[CVE-2015-2192](#)

### Уязвимость

Риск: Средний

ALT X ID  
65599

**Уязвимость в TN5250 диссекторе Wireshark 1.10.x до 1.10.11 и 1.12.x до 1.12.2 (CVE-2014-8714)**

### Описание

Функция `dissect_write_structured_field` в `epan/dissectors/packet-tn5250.c` в TN5250 диссекторе Wireshark 1.10.x до 1.10.11 и 1.12.x до 1.12.2 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (бесконечный цикл) через специально сформированный пакет.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

### Ссылки

**oval:ru.altx-soft.win:def:38041**

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38041>

### CVE-2014-8714 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-399

[CVE-2014-8714](#)

### Уязвимость

Риск: Средний

ALT X ID  
65600

**Множественные уязвимости доступа к освобожденной памяти в WCCP диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 (CVE-2015-0559)**

### Описание

Множественные уязвимости доступа к освобожденной памяти в `epan/dissectors/packet-wccp.c` в WCCP диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 позволяют удалённым злоумышленникам вызвать отказ в обслуживании (падение приложения) через специально сформированный пакет.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

### Ссылки

**oval:ru.altx-soft.win:def:38042**

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38042>

### CVE-2015-0559 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

[CVE-2015-0559](#)

Уязвимость

Риск: Средний

ALTX ID  
65597

**Уязвимость в NCP диссекторе Wireshark 1.10.x до 1.10.11 и 1.12.x до 1.12.2 (CVE-2014-8712)**

#### Описание

Функция build\_expert\_data в epan/dissectors/packet-ncp2222.inc в NCP диссекторе Wireshark 1.10.x до 1.10.11 и 1.12.x до 1.12.2 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (падение приложения) через специально сформированный пакет.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

#### Ссылки

oval:ru.altx-soft.win:def:38039

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38039>

### CVE-2014-8712 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-399

[CVE-2014-8712](#)

Уязвимость

Риск: Средний

ALTX ID  
65598

**Переполнение стека в NCP диссекторе Wireshark 1.10.x до 1.10.11 и 1.12.x до 1.12.2 (CVE-2014-8713)**

#### Описание

Переполнение стека в функции build\_expert\_data в epan/dissectors/packet-ncp2222.inc в NCP диссекторе Wireshark 1.10.x до 1.10.11 и 1.12.x до 1.12.2 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (падение приложения) через специально сформированный пакет.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

#### Ссылки

oval:ru.altx-soft.win:def:38040

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38040>

### CVE-2014-8713 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-119

[CVE-2014-8713](#)

Уязвимость

Риск: Средний

ALTX ID  
65601

**Уязвимость в WCCP диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 (CVE-2015-0560)**

#### Описание

Функция dissect\_wccp2r1\_address\_table\_info в epan/dissectors/packet-wccp.c в WCCP диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (падение приложения)

через специально сформированный пакет.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

#### Ссылки

**oval:ru.altx-soft.win:def:38043**

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38043>

#### CVE-2015-0560 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-19

[CVE-2015-0560](#)

Уязвимость

Риск: Средний

ALTX ID

65603

**Множественные уязвимости доступа к освобожденной памяти в DEC DNA Routing Protocol диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 (CVE-2015-0562)**

Описание

Множественные уязвимости доступа к освобожденной памяти в epan/dissectors/packet-dec-dnart.c в DEC DNA Routing Protocol диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 позволяют удалённым злоумышленникам вызвать отказ в обслуживании (падение приложения) через специально сформированный пакет.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

#### Ссылки

**oval:ru.altx-soft.win:def:38045**

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38045>

#### CVE-2015-0562 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

[CVE-2015-0562](#)

Уязвимость

Риск: Средний

ALTX ID

65604

**Уязвимость в SMTP диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 (CVE-2015-0563)**

Описание

SMTP диссектор Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (падение приложения) через специально сформированный пакет.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

#### Ссылки

**oval:ru.altx-soft.win:def:38046**

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38046>

#### CVE-2015-0563 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-20

[CVE-2015-0563](#)

**Уязвимость**

Риск: Средний

ALTX ID  
65602**Уязвимость в LPP диссекторе Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 (CVE-2015-0561)****Описание**

LPP диссектор Wireshark 1.10.x до 1.10.12 и 1.12.x до 1.12.3 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (доступ за пределами памяти и падение приложения) через специально сформированный пакет.

**Исправление**

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.wireshark.org/download.html>.

**Ссылки****oval:ru.altx-soft.win:def:38044**<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38044>**CVE-2015-0561 (CVE)**

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-20

[CVE-2015-0561](#)**Уязвимость**

Риск: Средний

ALTX ID  
58893**Уязвимость в SSL 3.0 (POODLE) в Internet Explorer (GPO) (CVE-2014-3566)****Описание**

Уязвимость в SSL 3.0, которая позволяет злоумышленникам получить доступ к передаваемым данным. Уязвимость получила наименование POODLE (Padding Oracle On Downgraded Legacy Encryption). Microsoft рекомендует отключить SSL 3.0 и включить TLS 1.0, TLS 1.1, and TLS 1.2 (<https://technet.microsoft.com/en-us/library/security/3009008.aspx>). Для настройки необходимо:

1. Открыть редактор групповых политик (gpedit.msc).
2. Перейти по пути: Конфигурация компьютера\Административные шаблоны\Компоненты Windows\Internet Explorer\Панель управления браузером\Вкладка "Дополнительно".
3. Выбрать "Выключить поддержку шифрования", нажать "Изменить".
4. Изменить сочетание безопасных протоколов на "Использовать TLS 1.0, TLS 1.1, и TLS 1.2".
5. Нажать "ОК".

**Исправление**

Необходимо произвести рекомендуемую производителем конфигурацию ПО в соответствии с инструкцией по ссылке <https://technet.microsoft.com/en-us/library/security/3009008.aspx>

**Ссылки****oval:ru.altx-soft.win:def:33596**<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:33596>**CVE-2014-3566 (CVE)**

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

CWE: CWE-310

[CVE-2014-3566](#)**Уязвимость**

Риск: Средний

ALTX ID  
72094**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3081)****Описание**

Уязвимость Race condition в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172,

позволяет удалённым злоумышленникам обойти механизм защиты Internet Explorer, посредством неопределённых векторов атаки.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

#### Ссылки

oval:ru.altx-soft.win:def:38988

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38988>

#### CVE-2015-3081 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

CWE: CWE-362

[CVE-2015-3081](#)

#### Уязвимость

Риск: Средний

ALTX ID  
72095

**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3082)**

#### Описание

Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет удалённым злоумышленникам обойти ограничения файловой системы операции записи, посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2015-3083 и CVE-2015-3085.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

#### Ссылки

oval:ru.altx-soft.win:def:38989

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38989>

#### CVE-2015-3082 (CVE)

CVSS: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:N/I:P/A:P)

CWE: CWE-264

[CVE-2015-3082](#)

#### Уязвимость

Риск: Средний

ALTX ID  
64306

**Неопределённая уязвимость в Schema Management компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0870)**

#### Описание

Неопределённая уязвимость в Schema Management компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25804

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25804>

#### CVE-2011-0870 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

[CVE-2011-0870](#)

<b>Уязвимость</b>	Риск: Средний
ALTX ID 72092	<b>Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3079)</b>
<b>Описание</b>	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет злоумышленникам обойти ограничения доступа и получить доступ к конфиденциальной информации посредством неопределённых векторов атаки.
<b>Исправление</b>	Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <a href="http://get.adobe.com/ru/flashplayer/">http://get.adobe.com/ru/flashplayer/</a> , <a href="http://get.adobe.com/ru/air/">http://get.adobe.com/ru/air/</a> .
<b>Ссылки</b>	<b>oval:ru.altx-soft.win:def:38986</b> <a href="http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38986">http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38986</a> <b>CVE-2015-3079 (CVE)</b> CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N) CWE: CWE-264 <a href="https://cve.mitre.org/cve/2015/3079/">CVE-2015-3079</a>

<b>Уязвимость</b>	Риск: Средний
ALTX ID 72096	<b>Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3083)</b>
<b>Описание</b>	Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет удалённым злоумышленникам обойти ограничения файловой системы операции записи, посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2015-3082 и CVE-2015-3085.
<b>Исправление</b>	Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <a href="http://get.adobe.com/ru/flashplayer/">http://get.adobe.com/ru/flashplayer/</a> , <a href="http://get.adobe.com/ru/air/">http://get.adobe.com/ru/air/</a> .
<b>Ссылки</b>	<b>oval:ru.altx-soft.win:def:38990</b> <a href="http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38990">http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38990</a> <b>CVE-2015-3083 (CVE)</b> CVSS: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:N/I:P/A:P) CWE: CWE-264 <a href="https://cve.mitre.org/cve/2015/3083/">CVE-2015-3083</a>

<b>Уязвимость</b>	Риск: Средний
ALTX ID 20373	<b>Уязвимость, приводящая к потреблению большого объема памяти (CVE-2013-1282)</b>
<b>Описание</b>	В реализациях Active Directory существует уязвимость, позволяющая заставить службу перестать отвечать на запросы. Данная уязвимость возникает, когда службе LDAP не удается обработать специально созданный запрос.
<b>Исправление</b>	Необходимо установить актуальное обновление от производителя.



#### Ссылки

oval:ru.altx-soft.win:def:17180

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:17180>

MS13-032 (Microsoft)

[MS13-032](#)

CVE-2013-1282 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CWE: CWE-20

[CVE-2013-1282](#)

#### Уязвимость

Риск: Средний

#### ALT X ID

72104

**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3091)**

#### Описание

Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, не должным образом ограничивает открытие адресов памяти, что позволяет удалённым злоумышленникам обойти защитный ASLR механизм посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2015-3092.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

#### Ссылки

oval:ru.altx-soft.win:def:38998

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38998>

CVE-2015-3091 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CWE: CWE-200

[CVE-2015-3091](#)

#### Уязвимость

Риск: Средний

#### ALT X ID

72098

**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3085)**

#### Описание

Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, позволяет удалённым злоумышленникам обойти ограничения файловой системы операции записи, посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2015-3082 и CVE-2015-3083.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

#### Ссылки

oval:ru.altx-soft.win:def:38992

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38992>

CVE-2015-3085 (CVE)

CVSS: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:N/I:P/A:P)

CWE: CWE-264

[CVE-2015-3085](#)

#### Уязвимость

Риск: Средний

ALTX ID

22840

**Уязвимость обхода безопасности в Microsoft Windows Human Interface Device (HID) драйвере (CVE-2011-0638)**

#### Описание

Microsoft Windows ненадлежащим образом предупреждает пользователя перед включением Human Interface Device (HID) дополнительной функциональности USB, что позволяет при содействии пользователя удалённым злоумышленникам выполнить произвольные программы через специально сформированные USB данные.

#### Исправление

Необходимо остановить и отключить автозапуск службы: имя - "hidserv", отображаемое имя - "Доступ к HID-устройствам" ("Human Interface Device Access")

#### Ссылки

oval:ru.altx-soft.win:def:22098

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22098>

#### CVE-2011-0638 (CVE)

CVSS: Базовая оценка 6.9 (AV:L/AC:M/Au:N/C:C/I:C/A:C)

CWE: CWE-16

[CVE-2011-0638](#)

Уязвимость

Риск: Средний

ALTX ID

69505

**Неопределённая уязвимость в Oracle Java SE 8u40 (CVE-2015-0470)**

#### Описание

Неопределённая уязвимость в Oracle Java SE 8u40 позволяет удалённым злоумышленникам повлиять на целостность посредством неопределённых векторов атаки, связанных с Hotspot.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

#### Ссылки

oval:ru.altx-soft.win:def:38765

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38765>

#### CVE-2015-0470 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

[CVE-2015-0470](#)

Уязвимость

Риск: Средний

ALTX ID

69506

**Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0477)**

#### Описание

Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 позволяет удалённым злоумышленникам повлиять на целостность посредством неопределённых векторов атаки, связанных с Beans.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

#### Ссылки

oval:ru.altx-soft.win:def:38766

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38766>

### CVE-2015-0477 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

[CVE-2015-0477](#)

Уязвимость

Риск: Средний

ALTX ID  
64300

**Узвимость внедрения SQL в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-3132)**

#### Описание

Узвимость внедрения SQL в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым авторизованным пользователям выполнить произвольные SQL запросы через векторы, с участием CREATE INDEX с CTXSYS.CONTEXT INDEXTYPE и DBMS\_STATS.GATHER\_TABLE\_STATS.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25798

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25798>

### CVE-2012-3132 (CVE)

CVSS: Базовая оценка 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

CWE: CWE-89

[CVE-2012-3132](#)

Уязвимость

Риск: Средний

ALTX ID  
64301

**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-3134)**

#### Описание

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым авторизованным пользователям повлиять на доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25799

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25799>

### CVE-2012-3134 (CVE)

CVSS: Базовая оценка 4 (AV:N/AC:L/Au:S/C:N/I:N/A:P)

[CVE-2012-3134](#)

Уязвимость

Риск: Средний

ALTX ID  
69507

**Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0478)**

#### Описание

Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 позволяет удалённым злоумышленникам повлиять на конфиденциальность через векторы, связанные с JCE.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию

программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

#### Ссылки

oval:ru.altx-soft.win:def:38767

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38767>

#### CVE-2015-0478 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

[CVE-2015-0478](#)

Уязвимость

Риск: Средний

ALTX ID

69512

**Неопределённая уязвимость в Oracle Java SE 8u40 (CVE-2015-0486)**

Описание

Неопределённая уязвимость в Oracle Java SE 8u40 позволяет удалённым злоумышленникам повлиять на конфиденциальность посредством неопределённых векторов атаки, связанных с развертыванием.

Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

#### Ссылки

oval:ru.altx-soft.win:def:38772

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38772>

#### CVE-2015-0486 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

[CVE-2015-0486](#)

Уязвимость

Риск: Средний

ALTX ID

69513

**Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0488)**

Описание

Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40, позволяет удалённым злоумышленникам повлиять на доступность через векторы, связанные с JSSE.

Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

#### Ссылки

oval:ru.altx-soft.win:def:38773

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38773>

#### CVE-2015-0488 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

[CVE-2015-0488](#)

Уязвимость

Риск: Средний

ALTX ID

69509

**Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 (CVE-2015-0480)**

Описание

Неопределённая уязвимость в Oracle Java SE 5.0u81, 6u91, 7u76, и 8u40 позволяет удалённым злоумышленникам

повлиять на целостность и доступность посредством неопределённых векторов атаки, связанных с Tools.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

#### Ссылки

**oval:ru.altx-soft.win:def:38769**

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38769>

**CVE-2015-0480 (CVE)**

CVSS: Базовая оценка 5.8 (AV:N/AC:M/Au:N/C:N/I:P/A:P)

[CVE-2015-0480](#)

Уязвимость

Риск: Средний

ALTX ID  
69511

**Неопределённая уязвимость в Oracle Java SE 7u76 и 8u40 (CVE-2015-0484)**

#### Описание

Неопределённая уязвимость в Oracle Java SE 7u76 и 8u40, позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2015-0492.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://www.oracle.com/technetwork/java/javase/downloads/index.html>.

#### Ссылки

**oval:ru.altx-soft.win:def:38771**

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38771>

**CVE-2015-0484 (CVE)**

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

[CVE-2015-0484](#)

Уязвимость

Риск: Средний

ALTX ID  
58892

**Уязвимость в SSL 3.0 (POODLE) в Windows (CVE-2014-3566)**

#### Описание

Уязвимость в SSL 3.0, которая позволяет злоумышленникам получить доступ к передаваемым данным. Уязвимость получила наименование POODLE (Padding Oracle On Downgraded Legacy Encryption). Microsoft рекомендует отключить SSL 3.0 и включить TLS 1.0, TLS 1.1, and TLS 1.2 (<https://technet.microsoft.com/en-us/library/security/3009008.aspx>).

#### Исправление

Необходимо произвести рекомендуемую производителем конфигурацию ПО в соответствии с инструкцией по ссылке <https://technet.microsoft.com/en-us/library/security/3009008.aspx>

#### Ссылки

**oval:ru.altx-soft.win:def:33595**

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:33595>

**CVE-2014-3566 (CVE)**

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:P/I:N/A:N)

CWE: CWE-310

[CVE-2014-3566](#)

Уязвимость

Риск: Средний

ALTX ID  
64263

**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0880)**

#### Описание

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25761

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25761>

**CVE-2011-0880 (CVE)**

CVSS: Базовая оценка 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

[CVE-2011-0880](#)

Уязвимость

Риск: Средний

ALTX ID  
64274

**Неопределённая уязвимость в Security Framework компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-2244)**

#### Описание

Неопределённая уязвимость в Security Framework компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым злоумышленникам повлиять на конфиденциальность и целостность посредством неопределённых векторов атаки, связанных с Authentication.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25772

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25772>

**CVE-2011-2244 (CVE)**

CVSS: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

[CVE-2011-2244](#)

Уязвимость

Риск: Средний

ALTX ID  
64262

**Неопределённая уязвимость в Instance Management компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0879)**

#### Описание

Неопределённая уязвимость в Instance Management компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым злоумышленникам повлиять на целостность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25760

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25760>

### CVE-2011-0879 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

[CVE-2011-0879](#)

Уязвимость

Риск: Средний

ALT X ID  
64257

**Неопределённая уязвимость в Security Framework компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0848)**

#### Описание

Неопределённая уязвимость в Security Framework компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки, связанных с User Model.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25755

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25755>

### CVE-2011-0848 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

[CVE-2011-0848](#)

Уязвимость

Риск: Средний

ALT X ID  
64260

**Неопределённая уязвимость в Enterprise Manager Console компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0876)**

#### Описание

Неопределённая уязвимость в Enterprise Manager Console компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым злоумышленникам повлиять на целостность посредством неопределённых векторов атаки, связанных с безопасностью.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25758

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25758>

### CVE-2011-0876 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

[CVE-2011-0876](#)

Уязвимость

Риск: Средний

ALT X ID  
64281

**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 и 11.2.0.2 (CVE-2011-3512)**

#### Описание

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 и 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность и целостность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25779

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25779>

#### CVE-2011-3512 (CVE)

CVSS: Базовая оценка 5.5 (AV:N/AC:L/Au:S/C:P/I:P/A:N)

[CVE-2011-3512](#)

#### Уязвимость

Риск: Средний

ALTX ID  
64282

**Неопределённая уязвимость в Listener компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 и 11.2.0.2 (CVE-2012-0072)**

#### Описание

Неопределённая уязвимость в Listener компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 и 11.2.0.2 позволяет удалённым злоумышленникам повлиять на доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25780

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25780>

#### CVE-2012-0072 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

[CVE-2012-0072](#)

#### Уязвимость

Риск: Средний

ALTX ID  
23191

**Уязвимость в Adobe Shockwave Player до 11.5.8.612 (CVE-2010-2865)**

#### Описание

Неопределённая уязвимость в Adobe Shockwave Player до 11.5.8.612 позволяет удалённым злоумышленникам вызвать отказ в обслуживании посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22457

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22457>

#### CVE-2010-2865 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

[CVE-2010-2865](#)

#### Уязвимость

Риск: Средний

ALTX ID  
64275

**Неопределённая уязвимость в SQL Performance Advisories/UIs компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-2248)**

#### Описание

Неопределённая уязвимость в SQL Performance Advisories/UIs компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность, связано



с SQL Details UI & Explain Plan.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:25773

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25773>

**CVE-2011-2248 (CVE)**

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

[CVE-2011-2248](#)

Уязвимость

Риск: Средний

ALTX ID  
64277

**Неопределённая уязвимость в Database Target Type Menus компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-2257)**

**Описание**

Неопределённая уязвимость в Database Target Type Menus компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:25775

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25775>

**CVE-2011-2257 (CVE)**

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

[CVE-2011-2257](#)

Уязвимость

Риск: Средний

ALTX ID  
64256

**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0838)**

**Описание**

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки, связанных с привилегией create procedure.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:25754

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25754>

**CVE-2011-0838 (CVE)**

CVSS: Базовая оценка 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

[CVE-2011-0838](#)

Уязвимость

Риск: Средний

ALTX ID 53417	<b>Уязвимость SQL Master Data Services, приводящая к межсайтовому выполнению сценариев (XSS) (CVE-2014-1820)</b>
------------------	--

**Описание**

В SQL Master Data Services (MDS) существует уязвимость, приводящая к межсайтовому выполнению сценариев (XSS), которая может позволить злоумышленнику внедрить сценарий на стороне клиента в пользовательском экземпляре Internet Explorer. Сценарий может подменить содержимое, раскрыть данные или предпринять любое действие, которое может осуществлять пользователь на сайте, от имени атакованного пользователя.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

**oval:ru.altx-soft.win:def:24101**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24101>

**CVE-2014-1820 (CVE)**

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

CWE: CWE-79

[CVE-2014-1820](#)

**MS14-044 (Microsoft)**

[MS14-044](#)

**Уязвимость**

Риск: Средний

ALTX ID 64249	<b>Неопределённая уязвимость в Network Foundation компоненте в Oracle Database Server 10.1.0.5, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0806)</b>
------------------	---

**Описание**

Неопределённая уязвимость в Network Foundation компоненте в Oracle Database Server 10.1.0.5, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым злоумышленникам повлиять на доступность посредством неопределённых векторов атаки.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

**oval:ru.altx-soft.win:def:25747**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25747>

**CVE-2011-0806 (CVE)**

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

[CVE-2011-0806](#)

**Уязвимость**

Риск: Средний

ALTX ID 53418	<b>Уязвимость Microsoft SQL Server, приводящая к переполнению стека (CVE-2014-4061)</b>
------------------	---

**Описание**

В SQL Server существует уязвимость, приводящая к отказу в обслуживании. Злоумышленник, успешно воспользовавшийся данной уязвимостью, может заставить сервер перестать отвечать на запросы, пока не будет инициирована ручная перезагрузка.

**Исправление**

Необходимо установить актуальное обновление от производителя.

#### Ссылки

**oval:ru.altx-soft.win:def:24102**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24102>

#### **CVE-2014-4061 (CVE)**

CVSS: Базовая оценка 6.8 (AV:N/AC:L/Au:S/C:N/I:N/A:C)

CWE: CWE-399

[CVE-2014-4061](#)

#### **MS14-044 (Microsoft)**

[MS14-044](#)

#### Уязвимость

Риск: Средний

#### ALTX ID

64355

**Уязвимость в Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356 (CVE-2014-8437)**

#### Описание

Adobe Flash Player до 13.0.0.252 и 14.x и 15.x до 15.0.0.223, Adobe AIR до 15.0.0.356, позволяет удалённым злоумышленникам discover session tokens посредством неопределённых векторов атаки.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/air/>, <http://get.adobe.com/ru/flashplayer/>.

#### Ссылки

**oval:ru.altx-soft.win:def:24653**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:24653>

#### **CVE-2014-8437 (CVE)**

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CWE: CWE-200

[CVE-2014-8437](#)

#### **aprb14-24 (Adobe)**

[aprb14-24](#)

#### Уязвимость

Риск: Средний

#### ALTX ID

64242

**Неопределённая уязвимость в Oracle Help компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1, 11.2.0.2, 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5 и 10.1.0.5 (CVE-2011-0785)**

#### Описание

Неопределённая уязвимость в Oracle Help компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1, 11.2.0.2, 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5 и 10.1.0.5 позволяет удалённым злоумышленникам повлиять на целостность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

**oval:ru.altx-soft.win:def:25740**

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25740>

#### **CVE-2011-0785 (CVE)**

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

[CVE-2011-0785](#)

#### Уязвимость

Риск: Средний

ALTX ID 23718	<b>Уязвимость в Adobe Shockwave Player до 11.5.7.609 (CVE-2010-1282)</b>
------------------	--

#### Описание

Adobe Shockwave Player до 11.5.7.609 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (бесконечный цикл и потребление CPU) посредством специально сформированного размера ATOM в .dir (aka Director) файле.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:22884

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:22884>

#### CVE-2010-1282 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:N/A:P)

CWE: CWE-399

[CVE-2010-1282](#)

Уязвимость	Риск: Средний
------------	---------------

ALTX ID 64255	<b>Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0835)</b>
------------------	---

#### Описание

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25753

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25753>

#### CVE-2011-0835 (CVE)

CVSS: Базовая оценка 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

[CVE-2011-0835](#)

Уязвимость	Риск: Средний
------------	---------------

ALTX ID 64254	<b>Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0832)</b>
------------------	---

#### Описание

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25752

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25752>

### CVE-2011-0832 (CVE)

CVSS: Базовая оценка 6 (AV:N/AC:M/Au:S/C:P/I:P/A:P)

[CVE-2011-0832](#)

Уязвимость

Риск: Средний

ALT X ID  
64251

**Неопределённая уязвимость в CMDB Metadata & Instance APIs компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0816)**

#### Описание

Неопределённая уязвимость в CMDB Metadata & Instance APIs компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность и целостность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25749

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25749>

### CVE-2011-0816 (CVE)

CVSS: Базовая оценка 5.5 (AV:N/AC:L/Au:S/C:P/I:P/A:N)

[CVE-2011-0816](#)

Уязвимость

Риск: Средний

ALT X ID  
64253

**Неопределённая уязвимость в Enterprise Config Management компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0831)**

#### Описание

Неопределённая уязвимость в Enterprise Config Management компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность и целостность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25751

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25751>

### CVE-2011-0831 (CVE)

CVSS: Базовая оценка 5.5 (AV:N/AC:L/Au:S/C:P/I:P/A:N)

[CVE-2011-0831](#)

Уязвимость

Риск: Средний

ALT X ID  
43542

**Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2013-1554)**

#### Описание

Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 позволяет удалённым злоумышленникам повлиять на доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:32437

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:32437>

#### CVE-2013-1554 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

[CVE-2013-1554](#)

Уязвимость

Риск: Средний

ALT X ID  
64295

**Неопределённая уязвимость в Enterprise Manager для Oracle Database компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-1737)**

#### Описание

Неопределённая уязвимость в Enterprise Manager для Oracle Database компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым злоумышленникам повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки, связанных с DB Performance Advisories/UIs.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25793

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25793>

#### CVE-2012-1737 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

[CVE-2012-1737](#)

Уязвимость

Риск: Средний

ALT X ID  
64296

**Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-1745)**

#### Описание

Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым злоумышленникам повлиять на доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25794

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25794>

#### CVE-2012-1745 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

[CVE-2012-1745](#)

Уязвимость

Риск: Средний

ALT X ID  
32981

**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2, 11.2.0.3, и 12.1.0.1 (CVE-2013-3826)**

#### Описание

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2, 11.2.0.3, и 12.1.0.1

позволяет удалённым злоумышленникам повлиять на конфиденциальность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:31397

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:31397>

#### CVE-2013-3826 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

[CVE-2013-3826](#)

#### Уязвимость

Риск: Средний

ALTX ID  
64293

**Неопределённая уязвимость в RDBMS Core компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-0534)**

#### Описание

Неопределённая уязвимость в RDBMS Core компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым авторизованным пользователям повлиять на целостность посредством неопределённых векторов атаки, связанных с Create Session.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25791

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25791>

#### CVE-2012-0534 (CVE)

CVSS: Базовая оценка 4 (AV:N/AC:L/Au:S/C:N/I:P/A:N)

[CVE-2012-0534](#)

#### Уязвимость

Риск: Средний

ALTX ID  
43536

**Уязвимость в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2012-3137)**

#### Описание

Протокол аутентификации в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 позволяет удалённым злоумышленникам получить ключ сессии и соль для произвольных пользователей, что упрощает проведение атаки полным перебором (brute force), используя информацию о криптографическом хэше.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:32431

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:32431>

#### CVE-2012-3137 (CVE)

CVSS: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)

CWE: CWE-287

[CVE-2012-3137](#)

#### Уязвимость

Риск: Средний

ALTX ID

64299

**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-1751)**

**Описание**

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:25797

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25797>

**CVE-2012-1751 (CVE)**

CVSS: Базовая оценка 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

[CVE-2012-1751](#)

Уязвимость

Риск: Средний

ALTX ID

43591

**Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 11.2.0.2 и 11.2.0.3 (CVE-2013-1538)**

**Описание**

Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 11.2.0.2 и 11.2.0.3 позволяет удалённым злоумышленникам повлиять на доступность посредством неопределённых векторов атаки.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:32487

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:32487>

**CVE-2013-1538 (CVE)**

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

[CVE-2013-1538](#)

Уязвимость

Риск: Средний

ALTX ID

43595

**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2013-3789)**

**Описание**

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность, целостность и доступность посредством неопределённых векторов атаки.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки**

oval:ru.altx-soft.win:def:32491

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:32491>



### CVE-2013-3789 (CVE)

CVSS: Базовая оценка 6.5 (AV:N/AC:L/Au:S/C:P/I:P/A:P)

[CVE-2013-3789](#)

Уязвимость

Риск: Средний

ALT X ID  
64297

**Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-1746)**

#### Описание

Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым злоумышленникам повлиять на доступность посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2012-1747.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25795

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25795>

### CVE-2012-1746 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

[CVE-2012-1746](#)

Уязвимость

Риск: Средний

ALT X ID  
72105

**Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172 (CVE-2015-3092)**

#### Описание

Уязвимость в Adobe Flash Player до 13.0.0.289 и 14.x по 17.x до 17.0.0.188, Adobe AIR до 17.0.0.172, не должным образом ограничивает открытие адресов памяти, что позволяет удалённым злоумышленникам обойти защитный ASLR механизм посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2015-3091.

#### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>, <http://get.adobe.com/ru/air/>.

#### Ссылки

oval:ru.altx-soft.win:def:38999

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:38999>

### CVE-2015-3092 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

CWE: CWE-200

[CVE-2015-3092](#)

Уязвимость

Риск: Средний

ALT X ID  
64298

**Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-1747)**

#### Описание

Неопределённая уязвимость в Network Layer компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым злоумышленникам повлиять на доступность посредством неопределённых векторов атаки. Уязвимость отлична от CVE-2012-1746.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25796

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25796>

#### CVE-2012-1747 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

[CVE-2012-1747](#)

#### Уязвимость

Риск: Средний

ALTX ID  
64288

**Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 и 11.2.0.2 (CVE-2012-0520)**

#### Описание

Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 и 11.2.0.2 позволяет удалённым злоумышленникам повлиять на целостность посредством неопределённых векторов атаки, связанных с безопасностью Framework.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25786

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25786>

#### CVE-2012-0520 (CVE)

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

[CVE-2012-0520](#)

#### Уязвимость

Риск: Средний

ALTX ID  
64289

**Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-0525)**

#### Описание

Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность и целостность посредством неопределённых векторов атаки, связанных с Enterprise Config Management.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25787

<http://www.ovaldb.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25787>

#### CVE-2012-0525 (CVE)

CVSS: Базовая оценка 4.9 (AV:N/AC:M/Au:S/C:P/I:P/A:N)

[CVE-2012-0525](#)

#### Уязвимость

Риск: Средний

ALTX ID  
64286

**Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 11.1.0.7 и 11.2.0.2 (CVE-2012-0512)**

### Описание

Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 11.1.0.7 и 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность и целостность посредством неопределённых векторов атаки, связанных с Enterprise Config Management.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:25784

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25784>

**CVE-2012-0512 (CVE)**

CVSS: Базовая оценка 5.5 (AV:N/AC:L/Au:S/C:P/I:P/A:N)

[CVE-2012-0512](#)

### Уязвимость

Риск: Средний

### ALT X ID

63829

**Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленнику получить доступ к конфиденциальной информации (CVE-2015-0302)**

### Описание

Adobe Flash Player до версии 13.0.0.260 и 14.x до 16.x до версии 16.0.0.257 в Windows позволяют злоумышленнику получить доступ к конфиденциальной информации посредством неопределённого вектора атаки.

### Исправление

Необходимо настроить автоматическое обновление, когда это возможно, либо вручную установить актуальную версию программы от производителя с сайта <http://get.adobe.com/ru/flashplayer/>.

### Ссылки

oval:ru.altx-soft.win:def:29537

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:29537>

**CVE-2015-0302 (CVE)**

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)

[CVE-2015-0302](#)

### Уязвимость

Риск: Средний

### ALT X ID

64283

**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-0082)**

### Описание

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым авторизованным пользователям повлиять на целостность и доступность посредством неопределённых векторов атаки.

### Исправление

Необходимо установить актуальное обновление от производителя.

### Ссылки

oval:ru.altx-soft.win:def:25781

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25781>

**CVE-2012-0082 (CVE)**

CVSS: Базовая оценка 5.5 (AV:N/AC:L/Au:S/C:N/I:P/A:P)

[CVE-2012-0082](#)

Уязвимость

Риск: Средний

ALTX ID  
64290

**Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-0526)**

#### Описание

Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым злоумышленникам повлиять на целостность посредством неопределённых векторов атаки, связанных с Schema Management.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25788

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25788>

**CVE-2012-0526 (CVE)**

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

[CVE-2012-0526](#)

Уязвимость

Риск: Средний

ALTX ID  
32978

**Неопределённая уязвимость в XML Parser компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2, 11.2.0.3, и 12.1.0.1 (CVE-2013-5771)**

#### Описание

Неопределённая уязвимость в XML Parser компоненте в Oracle Database Server 11.1.0.7, 11.2.0.2, 11.2.0.3, и 12.1.0.1 позволяет удалённым злоумышленникам повлиять на конфиденциальность и доступность посредством неопределённых векторов атаки.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:31392

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:31392>

**CVE-2013-5771 (CVE)**

CVSS: Базовая оценка 6.4 (AV:N/AC:L/Au:N/C:P/I:N/A:P)

[CVE-2013-5771](#)

Уязвимость

Риск: Средний

ALTX ID  
64291

**Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-0527)**

#### Описание

Неопределённая уязвимость в Enterprise Manager Base Platform компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым злоумышленникам повлиять на целостность посредством неопределённых векторов атаки, связанных с Schema Management.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25789

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25789>

**CVE-2012-0527 (CVE)**

CVSS: Базовая оценка 4.3 (AV:N/AC:M/Au:N/C:N/I:P/A:N)

[CVE-2012-0527](#)

Уязвимость

Риск: Низкий

ALTX ID  
64302**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 (CVE-2012-3146)****Описание**

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2 и 11.2.0.3 позволяет удалённым авторизованным пользователям повлиять на целостность посредством неопределённых векторов атаки.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:25800**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25800>**CVE-2012-3146 (CVE)**

CVSS: Базовая оценка 2.1 (AV:N/AC:H/Au:S/C:N/I:P/A:N)

[CVE-2012-3146](#)

Уязвимость

Риск: Низкий

ALTX ID  
43549**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 (CVE-2013-3790)****Описание**

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2, и 11.2.0.3 позволяет удалённым авторизованным пользователям повлиять на целостность посредством неопределённых векторов атаки.

**Исправление**

Необходимо установить актуальное обновление от производителя.

**Ссылки****oval:ru.altx-soft.win:def:32444**<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:32444>**CVE-2013-3790 (CVE)**

CVSS: Базовая оценка 2.1 (AV:N/AC:H/Au:S/C:N/I:P/A:N)

[CVE-2013-3790](#)

Уязвимость

Риск: Низкий

ALTX ID  
64247**Неопределённая уязвимость в Database Vault компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 (CVE-2011-0804)****Описание**

Неопределённая уязвимость в Database Vault компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.1 и 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на конфиденциальность и целостность посредством неопределённых векторов атаки.

**Исправление**

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25745

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25745>

#### CVE-2011-0804 (CVE)

CVSS: Базовая оценка 3.6 (AV:N/AC:H/Au:S/C:P/I:P/A:N)

[CVE-2011-0804](#)

#### Уязвимость

Риск: Низкий

ALTX ID  
64272

**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.2.0.1 и 11.2.0.2 (CVE-2011-2242)**

#### Описание

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.2.0.1 и 11.2.0.2 позволяет локальным пользователям повлиять на конфиденциальность, связано с XML DB FTP.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25770

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25770>

#### CVE-2011-2242 (CVE)

CVSS: Базовая оценка 1.3 (AV:L/AC:M/Au:M/C:P/I:N/A:N)

[CVE-2011-2242](#)

#### Уязвимость

Риск: Низкий

ALTX ID  
64280

**Неопределённая уязвимость в Database Vault компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 и 11.2.0.2 (CVE-2011-3511)**

#### Описание

Неопределённая уязвимость в Database Vault компоненте в Oracle Database Server 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7 и 11.2.0.2 позволяет удалённым авторизованным пользователям повлиять на целостность и доступность посредством неопределённых векторов атаки, связанных с Privileged Account.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

oval:ru.altx-soft.win:def:25778

<http://www.ovaldb.ru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25778>

#### CVE-2011-3511 (CVE)

CVSS: Базовая оценка 3.6 (AV:N/AC:H/Au:S/C:N/I:P/A:P)

[CVE-2011-3511](#)

#### Уязвимость

Риск: Низкий

ALTX ID  
64273

**Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7.3, 11.2.0.1 и 11.2.0.2 (CVE-2011-2243)**

#### Описание

Неопределённая уязвимость в Core RDBMS компоненте в Oracle Database Server 11.1.0.7.3, 11.2.0.1 и 11.2.0.2 позволяет

удалённым авторизованным пользователям повлиять на целостность, связано с SYSDBA.

#### Исправление

Необходимо установить актуальное обновление от производителя.

#### Ссылки

**oval:ru.altx-soft.win:def:25771**

<http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.win:def:25771>

**CVE-2011-2243 (CVE)**

CVSS: Базовая оценка 3.5 (AV:N/AC:M/Au:S/C:N/I:P/A:N)

[CVE-2011-2243](#)

---

Конец отчета. RedCheck 1.4.1.1.  
RedCheckID: 6DF9800A-476F-43D7-B922-36DDF894130F.  
© ЗАО "АЛТЭКС-СОФТ"