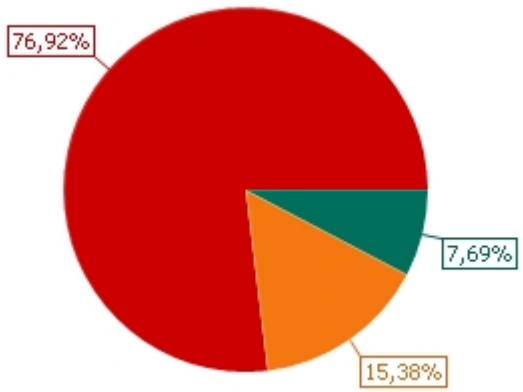
ALTEX SOFT

ОТЧЁТ

№ отчёта	*1d0cce2f-a34d-45d6-bdd9-60dd7e83d4f9*
Профиль	*Уязвимости*
Задание	*Job_4666*
Начало/завершение сканирования	*08.05.2015 15:48:31 / 08.05.2015 15:51:26*
Формирование отчёта	*19.05.2015 15:33:05*
Имя	*Quick_192.168.100.204_114*
Описание	*Автогенерируемый отчет вкладки "История" для "192.168.100.204" из "Job_4666" задания.*
Хосты [1]	*192.168.100.204*

Диаграмма распределения уязвимостей по уровням риска



Риск	*Количество*
Высокий	*10*
Средний	*2*
Низкий	*1*
Всего	*13*

Таблица распределения уязвимостей по хостам

Хост / Риск	Высокий	Средний	Низкий	Всего
192.168.100.204	*10*	*2*	*1*	*13*
Всего	**10**	**2**	**1**	**13**

Таблица распределения уязвимостей по продуктам

Продукт / Риск	Высокий	Средний	Низкий	Всего
cpe:/o:cisco:ios	*10*	*2*	*1*	*13*
Всего	**10**	**2**	**1**	**13**

Хост: 192.168.100.204

CPE	*cpe:/o:cisco:ios*
Начало/завершение сканирования	*08.05.2015 15:48:31 / 08.05.2015 15:51:26*
Профиль	*Имя профиля: cisco_stend* *Пароль "Enable": Да*
Агент	*Нет*
Тип сканирования	*Полное*
Уязвимостей найдено	***13:*** ***10*** ***2*** ***1***

Уязвимости [13]

Хост	ALTX ID	Риск	Название
192.168.100.204	63356	Высокий	Уязвимость в Cisco IOS Software Multiprotocol Label Switching Packet (CVE-2010-0576)
cpe:/o:cisco:ios			*major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)*
192.168.100.204	63532	Высокий	Уязвимость в Cisco IOS Secure Shell (CVE-2008-1159)
cpe:/o:cisco:ios			*major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)*
192.168.100.204	63325	Высокий	Уязвимость отказа службы инициализации протокола (CVE-2012-3949)
cpe:/o:cisco:ios			*major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)*
192.168.100.204	63515	Высокий	Уязвимость в Cisco Systems Non-DOCSIS Platform Default DOCSIS SNMP Support (CVE-2006-4950)
cpe:/o:cisco:ios			*major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)*
192.168.100.204	63395	Высокий	Уязвимость в Cisco IOS Software (CVE-2012-0386)
cpe:/o:cisco:ios			*show_subcommand=show ip ssh, config_line=SSH Enabled - version 2.0* *Authentication timeout: 120 secs; Authentication retries: 3*
			major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)
192.168.100.204	67367	Высокий	Уязвимость в Cisco IOS System Timers (CVE-2005-3481)
cpe:/o:cisco:ios			*major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)*
192.168.100.204	63544	Высокий	Уязвимость в Cisco IOS Firewall Authentication Proxy (CVE-2005-2841)
cpe:/o:cisco:ios			*major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)*
			show_subcommand=show running-config, config_line=Building configuration... *Current configuration : 1278 bytes* *!* *version 12.4* *service timestamps debug datetime msec* *service timestamps log datetime msec* *service password-encryption* *!* *hostname r2* *!* *boot-start-marker* *boot-end-marker* *!* *enable secret 5 1h0p2$sZbtAdmZ216CTs47A6KMv.* *enable password 7 051F031C35085E3E1D54* *!* *aaa new-model*

```
!
!
!
aaa session-id common
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip domain name dev.altx-soft.ru
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username user privilege 15 password 7 021201481F421F16481F
!
!
ip tcp synwait-time 5
ip ssh rsa keypair-name r2.dev.altx-soft.ru
ip ssh version 2
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.100.204 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
access-list 23 permit 192.168.100.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
control-plane
!
!
!
!
```

			! *!* *!* *!* *!* *!* *line con 0* *exec-timeout 0 0* *privilege level 15* *logging synchronous* *line aux 0* *exec-timeout 0 0* *privilege level 15* *logging synchronous* *line vty 0 4* *access-class 23 in* *exec-timeout 0 0* *logging synchronous* *transport input ssh* *!* *!* *end*
192.168.100.204	63562	Высокий	Уязвимость в provider-edge MPLS NAT реализации в Cisco IOS (CVE-2011-3279)
cpe:/o:cisco:ios			*major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)*
192.168.100.204	65858	Высокий	Уязвимость туннелей в Cisco IOS Software (CVE-2009-2873)
cpe:/o:cisco:ios			*major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)*
192.168.100.204	67366	Высокий	Уязвимость в Cisco IOS IPv4 (CVE-2007-0479)
cpe:/o:cisco:ios			*major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)*
192.168.100.204	63550	Средний	Уязвимость в Cisco Systems IPSec IKE (CVE-2005-3669)
cpe:/o:cisco:ios			*major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)*
192.168.100.204	63332	Средний	Уязвимость туннелей в Cisco IOS Software (CVE-2009-2872)
cpe:/o:cisco:ios			*major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)*
192.168.100.204	63538	Низкий	Уязвимость в Cisco Systems Internetwork Operating System IPv6 Packet (CVE-2005-2451)
cpe:/o:cisco:ios			*major_release=12.4(25), train_number=12.4, major_version=12, minor_version=4, release=25, train_identifier=mainline, rebuild=, subrebuild=, mainline_rebuild=, version_string=12.4(25)*
			show_subcommand=show running-config, config_line=Building configuration... *Current configuration : 1278 bytes* *!* *version 12.4* *service timestamps debug datetime msec* *service timestamps log datetime msec* *service password-encryption* *!* *hostname r2* *!* *boot-start-marker* *boot-end-marker* *!* *enable secret 5 1h0p2$sZbtAdmZ216CTs47A6KMv.* *enable password 7 051F031C35085E3E1D54* *!* *aaa new-model* *!* *!* *!* *aaa session-id common*

```
memory-size iomem 5
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
ip domain name dev.altx-soft.ru
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
!
username user privilege 15 password 7 021201481F421F16481F
!
!
ip tcp synwait-time 5
ip ssh rsa keypair-name r2.dev.altx-soft.ru
ip ssh version 2
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.100.204 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
access-list 23 permit 192.168.100.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
control-plane
!
!
!
!
!
!
!
!
```

```
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 access-class 23 in
 exec-timeout 0 0
 logging synchronous
 transport input ssh
!
!
end
```

Список уязвимостей

Уязвимость Риск: Высокий

ALTX ID	Уязвимость в Cisco IOS Firewall Authentication Proxy (CVE-2005-2841)
63544	

Описание

Переполнение буфера в Firewall Authentication Proxy для FTP и Telnet Sessions для Cisco IOS 12.2ZH и 12.2ZL, 12.3 и 12.3T, и 12.4 и 12.4T позволяет удалённым злоумышленникам вызвать отказ в обслуживании и выполнить произвольный код через специально сформированные учетные данные проверки подлинности пользователя.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1221

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1221

CVE-2005-2841 (CVE)

CVSS: Базовая оценка 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

CVE-2005-2841

cisco-sa-20050907-auth_proxy (Vendor Advisory)

cisco-sa-20050907-auth_proxy

Уязвимость Риск: Высокий

ALTX ID	Уязвимость в Cisco IOS System Timers (CVE-2005-3481)
67367	

Описание

Cisco IOS 12.0 по 12.4 позволяет удалённым злоумышленникам выполнить произвольный код через переполнение кучи в системных таймерах.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1264

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1264

CVE-2005-3481 (CVE)

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

CVE-2005-3481

cisco-sa-20051102-timers (Vendor Advisory)

cisco-sa-20051102-timers

Уязвимость Риск: Высокий

ALTX ID	Уязвимость в provider-edge MPLS NAT реализации в Cisco IOS (CVE-2011-3279)
63562	

Описание

Уязвимость в provider-edge MPLS NAT реализации в Cisco IOS 12.1 по 12.4 и 15.0 по 15.1, и IOS XE 3.1.xSG позволяет удалённым злоумышленникам вызвать отказ в обслуживании (перезагрузка устройства) через поврежденный SIP пакет на UDP порт 5060.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1239

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1239

CVE-2011-3279 (CVE)

CVSS: Базовая оценка 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

CWE: CWE-399

CVE-2011-3279

cisco-sa-20110928-nat (Vendor Advisory)

cisco-sa-20110928-nat

Уязвимость Риск: Высокий

ALTX ID 67366	**Уязвимость в Cisco IOS IPv4 (CVE-2007-0479)**

Описание

Утечка памяти в TCP listener в Cisco IOS 9.x, 10.x, 11.x, и 12.x позволяет удалённым злоумышленникам вызвать отказ в обслуживании через отправку специально сформированных TCP трафик.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1263

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1263

CVE-2007-0479 (CVE)

CVSS: Базовая оценка 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)

CVE-2007-0479

cisco-sa-20070124-crafted-tcp (Vendor Advisory)

cisco-sa-20070124-crafted-tcp

Уязвимость Риск: Высокий

ALTX ID 65858	**Уязвимость туннелей в Cisco IOS Software (CVE-2009-2873)**

Описание

Устройства Cisco, использующие подверженные уязвимости версии ОС, могут быть подвержены атаке типа "отказ в обслуживании", если настроены на работу с IP-туннелями и Cisco Express Forwarding.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1245

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1245

CVE-2009-2873 (CVE)

CVSS: Базовая оценка 7.1 (AV:N/AC:M/Au:N/C:N/I:N/A:C)

CVE-2009-2873

cisco-sa-20090923-tunnels (Vendor Advisory)

cisco-sa-20090923-tunnels

Уязвимость Риск: Высокий

ALTX ID	Уязвимость в Cisco IOS Secure Shell (CVE-2008-1159)
63532	

Описание

Множественные неопределённые уязвимости в SSH server в Cisco IOS 12.4 позволяет удалённым злоумышленникам вызвать отказ в обслуживании (перезагрузка устройства) посредством неопределённых векторов атаки.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1209
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1209

CVE-2008-1159 (CVE)
CVSS: Базовая оценка 7.1 (AV:N/AC:M/Au:N/C:N/I:N/A:C)
CVE-2008-1159

cisco-sa-20080521-ssh (Vendor Advisory)
cisco-sa-20080521-ssh

Уязвимость Риск: Высокий

ALTX ID	Уязвимость в Cisco IOS Software Multiprotocol Label Switching Packet (CVE-2010-0576)
63356	

Описание

Неопределённая уязвимость в Cisco IOS 12.0 по 12.4, IOS XE 2.1.x по 2.3.x до 2.3.2, и IOS XR 3.2.x по 3.4.3, когда Multiprotocol Label Switching (MPLS) и Label Distribution Protocol (LDP) включен, позволяет удалённым злоумышленникам вызвать отказ в обслуживании (перезагрузка устройства и перезагрузка процесса) через специально сформированный LDP пакет.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1033
http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1033

CVE-2010-0576 (CVE)
CVSS: Базовая оценка 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
CVE-2010-0576

cisco-sa-20100324-ldp (Vendor Advisory)
cisco-sa-20100324-ldp

Уязвимость Риск: Высокий

ALTX ID	Уязвимость отказа службы инициализации протокола (CVE-2012-3949)
63325	

Описание

Уязвимость в SIP реализации в Cisco Unified Communications Manager (CUCM) 6.x и 7.x до 7.1(5b)su5, 8.x до 8.5(1)su4, и 8.6 до 8.6(2a)su1; Cisco IOS 12.2 по 12.4 и 15.0 по 15.2; и Cisco IOS XE 3.3.xSG до 3.3.1SG, 3.4.xS, и 3.5.xS позволяет не прошедшему аутентификацию удаленному злоумышленнику вызывать сбой в работе критических служб, тем самым прерывая работу некоторых служб. Подверженные уязвимости устройства должны быть настроены на обработку SIP-сообщений для реализации этой уязвимости.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1002

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1002

CVE-2012-3949 (CVE)

CVSS: Базовая оценка 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
CWE: CWE-20
CVE-2012-3949

cisco-sa-20120926-cucm (Vendor Advisory)

cisco-sa-20120926-cucm

cisco-sa-20120926-sip (Vendor Advisory)

cisco-sa-20120926-sip

Уязвимость Риск: Высокий

ALTX ID 63395	**Уязвимость в Cisco IOS Software (CVE-2012-0386)**

Описание

Уязвимость в SSHv2 реализации в Cisco IOS 12.2, 12.4, 15.0, 15.1, и 15.2 и IOS XE 2.3.x по 2.6.x и 3.1.xS по 3.4.xS до 3.4.2S позволяет удалённым злоумышленникам вызвать отказ в обслуживании (перезагрузка устройства).

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1072

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1072

CVE-2012-0386 (CVE)

CVSS: Базовая оценка 7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
CWE: CWE-310
CVE-2012-0386

cisco-sa-20120328-ssh (Vendor Advisory)

cisco-sa-20120328-ssh

Уязвимость Риск: Высокий

ALTX ID 63515	**Уязвимость в Cisco Systems Non-DOCSIS Platform Default DOCSIS SNMP Support (CVE-2006-4950)**

Описание

Cisco IOS 12.2 по 12.4 позволяет удалённым злоумышленникам получить доступ на чтение и запись.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1192

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1192

CVE-2006-4950 (CVE)

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

CVE-2006-4950

cisco-sa-20060920-docsis (Vendor Advisory)

cisco-sa-20060920-docsis

Уязвимость Риск: Средний

ALTX ID 63332	**Уязвимость туннелей в Cisco IOS Software (CVE-2009-2872)**

Описание

Устройства Cisco, использующие подверженные уязвимости версии ОС, могут быть подвержены атаке типа "отказ в обслуживании", если настроены на работу с IP-туннелями и Cisco Express Forwarding.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1009

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1009

CVE-2009-2872 (CVE)

CVSS: Базовая оценка 6.8 (AV:N/AC:L/Au:S/C:N/I:N/A:C)

CVE-2009-2872

cisco-sa-20090923-tunnels (Vendor Advisory)

cisco-sa-20090923-tunnels

Уязвимость Риск: Средний

ALTX ID 63550	**Уязвимость в Cisco Systems IPSec IKE (CVE-2005-3669)**

Описание

Множественные неопределённые уязвимости в Internet Key Exchange version 1 (IKEv1) реализации во многих Cisco продуктах позволяет удалённым злоумышленникам вызвать отказ в обслуживании через некоторые поврежденные IKE пакеты.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1227

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1227

CVE-2005-3669 (CVE)

CVSS: Базовая оценка 5 (AV:N/AC:L/Au:N/C:N/I:N/A:P)

CVE-2005-3669

cisco-sa-20051114-ipsec (Vendor Advisory)

cisco-sa-20051114-ipsec

Уязвимость Риск: Низкий

ALTX ID 63538	**Уязвимость в Cisco Systems Internetwork Operating System IPv6 Packet (CVE-2005-2451)**

Описание

Cisco IOS 12.0 по 12.4 и IOS XR до 3.2 с IPv6, позволяет удалённым злоумышленникам в сегменте локальной сети вызвать отказ в обслуживании (перезагрузка устройства) и выполнить произвольный код через специально сформированный IPv6 пакет.

Исправление

Необходимо установить актуальное обновление от производителя.

Ссылки

oval:ru.altx-soft.cisco:def:1215

http://www.ovaldbru.altx-soft.ru/Definition.aspx?id=oval:ru.altx-soft.cisco:def:1215

CVE-2005-2451 (CVE)

CVSS: Базовая оценка 2.1 (AV:L/AC:L/Au:N/C:N/I:N/A:P)

CVE-2005-2451

cisco-sa-20050729-ipv6 (Vendor Advisory)

cisco-sa-20050729-ipv6

Конец отчета. RedCheck 1.4.1.1.
RedCheckID: 6DF9800A-476F-43D7-B922-36DDF894130F.
© ЗАО "АЛТЭКС-СОФТ"