RED Check

ОТЧЁТ

№ отчёта	*fc2bc8f3-720a-417d-95bb-57e66d69ab8c*
Профиль	*Конфигурации*
Задание	*Job_7042*
Начало/завершение сканирования	*29.07.2019 17:39:56 / 29.07.2019 17:40:44*
Формирование отчёта	*29.07.2019 17:42:18*
Имя	*Quick_192.168.100.162_118*
Описание	*Автогенерируемый отчет вкладки "История" для "192.168.100.162" из "Job_7042" задания.*
Хосты [1]	*192.168.100.162*

Сводная таблица результатов сканирования

Хост	Конфигурация	Всего	Соответствие
192.168.100.162	Конфигурация безопасности «Хост VMware ESXi 6»	65	13

Хост: 192.168.100.162

CPE	*cpe:/o:vmware:esxi_server:6.0*
Начало/завершение сканирования	*29.07.2019 17:39:56 / 29.07.2019 17:40:44*
Учетные данные	*Имя профиля: eee* *Тип: VMware*
Метод получения данных	*Безагентный механизм*

Конфигурация безопасности «Хост VMware ESXi 6» (профиль: Конфигурация безопасности «Хост VMware ESXi 6»)

Конфигурация не соответствует эталонной. Всего - 65, соответствие - 13 (20 %)

Соответствие (13) **Несоответствие (51)** **Не проверено (1)**

VMware ESXi 6

ESXi хосты

- Включить строгий Lockdown Mode для ограничения доступа
  Критичность: *Высокий*
- Значение Image Profile и VIB Acceptance Levels - VMware Certified
  Критичность: *Высокий*
- Ограничить непредусмотренное использование dvfilter сетевых API
  Критичность: *Высокий*
- Включить BPDU фильтр для ESXi хоста для предотвращения блокировки физических портов коммутатора с включёнными PortFast и BPDU Guard
  Критичность: *Высокий*
- Аудит пользователей из списка исключений, которые имеют административные привилегии
  Критичность: *Высокий*
- Настроить синхронизацию времени NTP
  Критичность: *Высокий*
- Настроить постоянное логирование для всех ESXi хостов
  Критичность: *Высокий*
- Настроить правильную конфигурацию SNMP
  Критичность: *Высокий*
- Отключить Managed Object Browser (MOB)
  Критичность: *Высокий*
- Использовать Active Directory для аутентификации локального пользователя
  Критичность: *Высокий*
- Настроить удаленное логирование для ESXi хостов
  Критичность: *Высокий*
- Отключить SSH
  Критичность: *Высокий*
- Отключить ESXi Shell
  Критичность: *Высокий*
- Настроить брандмауэр ESXi хоста на ограничение доступа к службам, запущенным на хосте
  Критичность: *Высокий*
- Настроить время до автоматической разблокировки заблокированной учетной записи
  Критичность: *Высокий*

- Настроить количество неудачных попыток входа в систему до блокировски учётной запсии
  Критичность: Высокий
- Настроить DCUI.Access для довереных пользователей
  Критичность: Высокий
- Настроить DCUI таймаут
  Критичность: Высокий
- Создать политику паролей
  Критичность: Высокий
- Настроить время простоя до автоматического прекращения ESXi Shell и SSH сессий
  Критичность: Высокий
- Настроить время работы служб SSH и ESXi Shell
  Критичность: Высокий
- Настроить intra-VM TPS
  Критичность: Высокий
- Система ESXi полностью обновлена
  Критичность: Высокий

Виртуальные машины

- **Отключить в явном виде операции копировать/вставить**
  - Отключить операцию копирования
    Критичность: Высокий
  - Отключить операцию перетаскивания
    Критичность: Высокий
  - Отключить параметр setGUIOptions
    Критичность: Высокий
  - Отключить операцию вставки
    Критичность: Высокий
- **Отключить сжатие/очистку виртуального диска**
  - Отключить сжатие виртуального диска
    Критичность: Высокий
  - Отключить очистку виртуального диска
    Критичность: Высокий
- **Отключить неэкспонированные функции**
  - Отключить autologon
    Критичность: Высокий
  - Отключить biosbbs
    Критичность: Высокий
  - Отключить getcreds
    Критичность: Высокий
  - Отключить launchmenu
    Критичность: Высокий
  - Отключить memsfss
    Критичность: Высокий
  - Отключить protocolhandler
    Критичность: Высокий
  - Отключить shellaction
    Критичность: Высокий
  - Отключить toporequest
    Критичность: Высокий

- Отключить trashfolderstate
  Критичность: Высокий
- Отключить trayicon
  Критичность: Высокий
- Отключить unity
  Критичность: Высокий
- Отключить unity interlock
  Критичность: Высокий
- Отключить unitypush
  Критичность: Высокий
- Отключить unity taskbar
  Критичность: Высокий
- Отключить unity unityactive
  Критичность: Высокий
- Отключить unity windowcontents
  Критичность: Высокий
- Отключить versionget
  Критичность: Высокий
- Отключить versionset
  Критичность: Высокий

Отключить посторонние устройства

- Отключить floppy устройства
  Критичность: Высокий
- Отключить parallel устройства
  Критичность: Высокий
- Отключить serial устройства
  Критичность: Высокий

Предотвратить несанкционированное удаление, изменение устройства и подключение к нему

- Запретить несанкционированное подключение устройств
  Критичность: Высокий
- Запретить несанкционированное модификацию устройств
  Критичность: Высокий

- Отключить передачу файлов HGFS
  Критичность: Высокий
- Отменить использование independent nonpersistent дисков
  Критичность: Высокий
- Отключить VIX сообщения от виртуальной машины
  Критичность: Высокий
- Отключить автоустановку
  Критичность: Высокий
- Ограничить объём VMX файла с информационными сообщениями от виртуальной машины
  Критичность: Высокий
- Контролировать доступ к консоли виртуальной машины через VNC протокол
  Критичность: Высокий
- Отключить отправку информации о хосте гостю
  Критичность: Высокий
- Проверить доступность виртуальной машины с присвоенной солью, которая совместно использует страницы памяти
  Критичность: Высокий

- Контролировать доступ к виртуальной машине через dvfilter network API
  Критичность: Высокий
- Контролировать использование функционала проброса PCI или PCIe
  Критичность: Высокий

vNetwork

- Политика “Forged Transmits” отключена
  Критичность: Высокий
- Политика “MAC Address Changes” отключена
  Критичность: Высокий
- Политика “Promiscuous Mode” отключена
  Критичность: Высокий

Описание параметров

Группа	
Название	**VMware ESXi 6**
Описание	

VMware ESXi является гипервизором нового поколения, не зависящим от операционной системы. Гипервизор VMware ESXi позволяет организовать оперативную работу центров обработки данных, обеспечивая повышенную безопасность, надежность и управляемость (доступен также в виде системы, встроенной в серверное аппаратное обеспечение).

Группа	
Название	**ESXi хосты**
Описание	

Настройки ESXi хостов.

Параметр	
Название	**Включить строгий Lockdown Mode для ограничения доступа**
Описание	

Эталонное значение: **Строгий**

В строгом режиме блокировки служба DCUI остановлена. Если подключение к серверу vCenter теряется и доступ через веб-клиент VMware vSphere закрыт, то ESXi хост становится недоступным, пока службы ESXi Shell и SSH остановлены и не определен список исключений пользователей. Если вы не можете восстановить соединение с vCenter, то необходимо переустановить хост.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Security Profile" ("Security and users" в 6.7). Пролистайте до "Lockdown Mode". Нажмите "Edit" и затем выберите "Strict".

Параметр	
Название	**Значение Image Profile и VIB Acceptance Levels - VMware Certified**
Описание	

Эталонное значение: **VMware Certified**

VIB со значением VMware Certified имеет самые строгие требования. VIB с этим уровнем проходит тщательное тестирование полностью эквивалентно VMware in-house Quality Assurance testing для той же технологии. VMware принимает обращения "VMware Certified" по технической поддержке самостоятельно.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Security Profile" ("Security and users" в 6.7). Пролистайте до "Host Image Profile Acceptance Level" ("Acceptance Level" в 6.7). Нажмите "Edit" и настройте "Acceptance Level" значение "VMware Certified".

Параметр	
Название	**Ограничить непредусмотренное использование dvfilter сетевых API**
Описание	

Эталонное значение: **Null**

Если вы не используете продукты, которым необходимы dvfilter сетевые API, то хост не должен быть настроен на отправку информации о сети на виртуальной машине. Если API включен, злоумышленник может попытаться подключить виртуальную машину к нему, тем самым потенциально обеспечивая доступ к сети других виртуальных машин хоста. Если вы используете продукт, которому необходим этот API, то убедитесь, что хост правильно настроен.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Advanced System Settings" ("System" -> "Advanced settings" в 6.7). Отфильтруйте по Net.DVFilterBindIpAddress. Нажмите edit и настройте его равном Null или IP-адресу соответствующей виртуальной машины с помощью dvfilter сетевых API.

	Параметр
Название	**Включить BPDU фильтр для ESXi хоста для предотвращения блокировки физических портов коммутатора с включёнными PortFast и BPDU Guard**
Описание	

Эталонное значение: **1**

BPDU Guard и Portfast обычно включены в физическом коммутаторе, к которому ESXi хост непосредственно подключен для уменьшения задержки конвергенции STP. Если пакет BPDU отправка с виртуальной машины ESXi хоста на физический коммутатор настроена, то может произойти каскадная блокировка всех интерфейсов восходящей линии от ESXi хоста. Для предотвращения этой блокировки BPDU фильтр может быть включен в ESXi хост, чтобы отказаться от каких-либо BPDU пакетов, отправляемых на физический коммутатор. Проблема заключается в том, что SSL VPN, который использует «подключения типа мост» Windows, может законно генерировать пакеты BPDU. Администратор должен убедиться в том, что нет никаких законных BPDU пакетов, сгенерённых виртуальными машинами хоста ESXi перед включением BPDU фильтра. Если BPDU фильтр включен в этой ситуации, то включение Reject Forged Transmits в виртуальных коммутаторах обеспечивает защиту от Spanning Tree петель.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Advanced System Settings" ("System" -> "Advanced settings" в 6.7). Отфильтруйте по Net.BlockGuestBPDU и проверьте,что значение равно 1.

	Параметр
Название	**Аудит пользователей из списка исключений, которые имеют административные привилегии**
Описание	

Эталонное значение: **Не пустой список**

В VMware vSphere 6.0 и более поздних версиях можно добавлять пользователей в список исключений пользователей из VMware vSphere Web Client. Эти пользователи не теряют свои разрешения, когда хост переходит в режим блокировки. Как правило, вы можете захотеть добавить учетные записи служб, таких как резервный агент в список исключений пользователей. Убедитесь в том, что список пользователей, которые освобождаются от потери разрешений является законным и в необходим в вашей среде. Пользователи, которые не требуют специальных разрешений, не должны быть освобождены от режима блокировки.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Security Profile" ("Security and users" в 6.7). Пролистайте до "Lockdown Mode". Нажмите "Edit" и затем нажмите "Exception Users". Добавьте или удалите пользователей в соответствии с требованиями сайта.

	Параметр
Название	**Настроить синхронизацию времени NTP**
Описание	

Эталонное значение: **Настроен**

Гарантируя, что все системы используют один и тот же относительный источник времени (включая соответствующее смещение локализации) и что относительный источник времени может быть соотнесен с согласованным стандартом времени (например, всемирное координированное время utc), вы можете упростить операцию отслеживания и соотнещения действий злоумышленника при рассмотрении соответствующих логов. Неверные настройки времени могут затруднить осмотр и соотношение лог-файлов, что помешает обнаружению атак и может сделать аудит некорректным.

Исправление

В веб-клиенте VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings". В "System Section" выберите "Time Configuration" ("Time and date" в 6.7), нажмите "Edit". Выберите "Use Network Time Protocol" (Enable NTP client), настройте политику запуска службы NTP, введите IP-адреса серверов NTP, с которыми синхронизироваться, нажмите Start или Restart.

	Параметр
Название	**Настроить постоянное логирование для всех ESXi хостов**
Описание	

Эталонное значение: **Настроен**

ESXi может быть сконфигурирован для хранения лог-файлов в файловую систему в памяти. Это происходит, когда каталог хоста "/scratch" связан с "/tmp/scratch". Тогда только логи за день будут храниться в любое время. Кроме того файлы журналов будут переинициализированы при каждой перезагрузке. Это представляет угрозу безопасности, так как активность пользователя хранятся временно и исчезнет после перезагрузки. Это также может усложнить аудит и усложнить отслеживание развития событий и диагностику проблем. Логирование ESXi хоста всегда должно быть настроено на постоянное хранилище данных.

Исправление

1. Определите путь к хранилищу данных, где вы хотите поместить лог, а затем войти в VMware vSphere Web Client.
2. Перейдите к хосту и выберите "Manage" ("Configure" в 6.5, "Edit" в 6.7) ("Configure" в 6.5, "Edit" в 6.7) и выберите "Advanced System Settings" ("System" -> "Advanced settings" в 6.7)
3. Введите "Syslog.global.LogDir" в фильтре, введите в качестве значения "Syslog.global.LogDir" выбранную директорию. Измените директорию по умолчанию (/tmp/scratch)!

Примечание: Syslog.global.LogDir должен быть настроен для каждого хоста.

	Параметр
Название	**Настроить правильную конфигурацию SNMP**
Описание	

Эталонное значение: **site-specific**

Если SNMP не используется, он должен быть выключен. Если он используется, то SNMP-ловушки должен быть настроены. Если SNMP не настроен должным образом, то информация о мониторинге может быть отправлена на вредоносный хост, который может затем использовать эту информацию для планирования атаки.
Примечание: ESXi 5.1 и более поздние версии поддерживает SNMPv3, что обеспечивает более высокий уровень безопасности, чем SNMPv1 или SNMPv2, в том числе ключей шифрования и аутентификации.

Исправление

Не настраивайте SNMP агент с VMware vSphere Web Client. Используйте esxcli, PowerCLI, или VMware vSphere Web Services SDK.

	Параметр
Название	**Отключить Managed Object Browser (MOB)**
Описание	

Эталонное значение: **False**

Managed Object Browser (MOB) предоставляет способ для изучения объектной модели, используемой VMkernel для управления хостом; для изменения конфигурации. Этот интерфейс предназначен для использования в первую очередь для отладки VMware vSphere SDK. В Sphere 6.0 этот параметр отключён по умолчанию.

Исправление

Откройте Web-клиент, Выберите "Settings" у хоста, далее "Advanced System Settings", найдите "Config.HostAgent.plugins.solo.enableMob" и настройте в "False".

	Параметр
Название	**Использовать Active Directory для аутентификации локального пользователя**
Описание	

Эталонное значение: **Настроен**

Добавьте ESXi хост к домену Active Directory (AD), чтобы устранить необходимость создания и поддержки нескольких локальных учетных записей пользователей. Использование AD для аутентификации пользователя упрощает конфигурацию ESXi хоста, обеспечивает повторное использование политик сложности пароля и снижает риск нарушений безопасности и несанкционированного доступа.
Примечание: если группа AD "ESX Admins" (по умолчанию) существует, то все пользователи и группы, которые назначены в качестве членов этой группы, будут иметь полный доступ ко всем ESXi хостам домена.

Исправление

В VMware vSphere Web Client выберите хост и перейдите в "Manage" -> "Authentication Services" ("Security and users" -> "Authentication" в 6.7), нажмите кнопку "Join Domain"". Укажите имя домена вместе с учетными данными для пользователя AD, которые имеет право на присоединение компьютера к домену.
Примечание:
(1) Вы можете использовать Host Profiles для автоматизации добавления хостов в домен AD. (2) Рассмотрите возможность использования прокси-сервера VMware vSphere Authentication, чтобы избежать передачи учетных данных AD по сети. Обратитесь к "enable-auth-proxy" рекомендации для получения дополнительной информации.

	Параметр
Название	**Настроить удаленное логирование для ESXi хостов**
Описание	

Эталонное значение: **Настроен**

Удаленное логирование на центральном хосте обеспечивает безопасное, централизованное хранилище для логов ESXi. Собрав все логи на центральном хосте, вы можете легко контролировать все хосты с помощью одного инструмента. Вы также можете обнаружить скоординированные атаки на нескольких хостах. Логирование в защищенный, централизованный сервер помогает предотвратить фальсификацию лога и обеспечивает запись долгосрочного аудита. Для облегчения удаленного ведения лога VMware предоставляет VMware vSphere Syslog Collector.

Исправление

1: Установка/Включение системного журнала хоста (vSphere Syslog Collector рекомендуется).
2: В веб-клиенте VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Advanced Sytem Settings" ("System" -> "Advanced settings" в 6.7), введите "Syslog.global.logHost" в фильтре, настройте "Syslog.global.logHost" на имя хоста вашего сервера с системными логами.

Примечание: при настройке удаленного лога хоста также рекомендуется настроить параметр "Syslog.global.logDirUnique" со значением True. Необходимо настроить параметры системного лога для каждого хоста. Параметры хоста системного журнала также можно настроить на vCLI, PowerCLI или с помощью API client.

	Параметр
Название	**Отключить SSH**

Описание

Эталонное значение: **False**

Этот сервис отключён по умолчанию.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Security Profile" ("Security and users" в 6.7). Пролистайте до "Services". Нажмите "Edit" и затем нажмите "SSH". Нажмите кнопку "stop".

	Параметр
Название	**Отключить ESXi Shell**

Описание

Эталонное значение: **False**

Этот сервис отключён по умолчанию.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Security Profile" ("Security and users" в 6.7). Пролистайте до "Services".Нажмите "Edit" и затем нажмите "ESXi Shell". Нажмите кнопку "stop".

	Параметр
Название	**Настроить брандмауэр ESXi хоста на ограничение доступа к службам, запущенным на хосте**

Описание

Эталонное значение: **Настроен**

Неограниченный доступ к службам, запущенным на ESXi хосте может открыть хост для внешних атак и несанкционированного доступа. Снижение риска путем настройки брандмауэра ESXi, чтобы разрешить доступ из авторизованных сетей.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Security Profile" ("Security and users" в 6.7).
Для каждого разрешенной службы как для входящих так и для исходящих подключений настройте подходящий сеть или IP-адрес после удаления флажка из "Allow connections from any IP address".

	Параметр
Название	**Настроить время до автоматической разблокировки заблокированной учетной записи**

Описание

Эталонное значение: **900**

Несколько неудачных попыток входа в систему представляют угрозу перебора пароля или вызвать отказ в обслуживании. Такие попытки перебора пароля должны быть ограничены путём блокировки учетной записи после достижения порогового значения.
В случае, если вы хотите автоматически разблокировать учётную запись, т.е. разблокировать учетную запись без административных действий, настройте время, в течение которого учетная запись остается заблокированной. Устанавливая большой период блокировки, вы будете сдерживать и серьезно замедлять метод перебора пароля.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" ->

"Advanced Sytem Settings" ("System" -> "Advanced settings" в 6.7). Введите "Security.AccountUnlockTime", нажмите edit и настройте значение 900.

	Параметр
Название	**Настроить количество неудачных попыток входа в систему до блокировски учётной запсии**
Описание	

Эталонное значение: **3**

Несколько неудачных попыток входа в систему представляют угрозу перебора пароля или вызвать отказ в обслуживании. Такие попытки перебора пароля должны быть ограничена путём блокировки учетной записи после достижения порогового значения.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Advanced Sytem Settings" ("System" -> "Advanced settings" в 6.7). Введите "Security.AccountLockFailures", нажмите edit и настройте значение 3.

	Параметр
Название	**Настроить DCUI.Access для довереных пользователей**
Описание	

Эталонное значение: **Список доверенных пользователей**

Lockdown режим отключает прямой доступ к хосту (администраторы могут управлять хостом из vCenter Server). Если хост становится изолированным от vCenter Server, администратор блокируется и больше не может управлять хостом. Если вы используете нормальный режим блокировки, вы можете избежать блокировки ESXi хоста, который работает в режиме блокировки, с помощью настройки DCUI.Access (добавление в список доверенных пользователей тех, которые могут переопределить режим блокировки доступа к DCUI). DCUI не работает в строгом режиме блокировки.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Advanced Sytem Settings" ("System" -> "Advanced settings" в 6.7). Введите "DCUI.Access", далее введите пользователей через запятую, у которых будет доступ к DCUI даже в режиме блокировки.
Предупреждение: Не удаляйте root.

	Параметр
Название	**Настроить DCUI таймаут**
Описание	

Эталонное значение: **600**

DCUI используется для непосредственного входа в ESXi хост и управления хостом. Подключение к DCUI должно быть прекращено после определённого временного промежутка, чтобы избежать непреднамеренного использования DCUI в оставшемся сеансе входа в систему.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Advanced Sytem Settings" ("System" -> "Advanced settings" в 6.7). Введите "UserVars.DcuiTimeOut" и настройте значение 600.

	Параметр
Название	**Создать политику паролей**

Описание

Эталонное значение: **По умолчанию**

ESXi хост использует pam_passwdqc.so плагин для настройки надежности и сложности пароля. Важно использовать пароли, которые сложно отгадываются и подбираются в генераторе паролей. Надёжность и сложность пароля применяются ко всем пользователям ESXi хоста, включая root. Они не применяются к пользователям Active Directory, когда хост ESX присоединен к домену, т.к. эти политики паролей включены в AD.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Advanced System Settings" ("System" -> "Advanced settings" в 6.7). Отфильтруйте по Security.PasswordQualityControl, оставте значение по умолчанию или усложните настройку.

	Параметр
Название	**Настроить время простоя до автоматического прекращения ESXi Shell и SSH сессий**

Описание

Эталонное значение: **900**

Если пользователь забыл выйти из SSH сессии, то соединение будет остается открытым на неопределенное время, увеличивая злоумышленнику возможность получить привилегированный доступ к хосту. ESXiShellInteractiveTimeOut позволяет автоматически прекратить бездействие сеанса.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Advanced System Settings" ("System" -> "Advanced settings" в 6.7). Отфильтруйте по UserVars.ESXiShellInteractiveTimeOut, оставте значение по умолчанию или усложните настройку.

	Параметр
Название	**Настроить время работы служб SSH и ESXi Shell**

Описание

Эталонное значение: **900**

Когда ESXi Shell или SSH службы включены, хост, к которому они подключены, будет работать бесконечно. Чтобы этого избежать, настройте ESXiShellTimeOut. ESXiShellTimeOut определяет время, по истечении которого будет автоматически разорвано соединение по SSH и ESXi Shell.

Исправление

Из веб-клиента VMware vSphere выберите хост, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Advanced System Settings" ("System" -> "Advanced settings" в 6.7). Отфильтруйте по UserVars.ESXiShellTimeOut, оставте значение по умолчанию или усложните настройку.

	Параметр
Название	**Настроить intra-VM TPS**

Описание

Эталонное значение: **2**

Существует научное исследование, в котором используется Transparent Page Sharing (TPS) для получения несанкционированного доступа к данным в рамках предупредительной меры ограничения TPS для отдельных виртуальных машин в новых версиях ESXi. Однако, компания VMware считает, что опубликованное раскрытие информации в связи с TPS между виртуальными машинами является непрактичным в реальном мира.
Виртуальные машины, которые не имеют настройки sched.mem.pshare.salt не могут совместно использовать память с любыми другими виртуальными машинами.

Исправление

Из веб-клиента VMware vSphere выберите хост и затем нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "System" -> "Advanced System Settings" ("System" -> "Advanced settings" в 6.7). Отфильтруйте по Mem.ShareForceSalting. Нажмите edit и настройте значение равным 2.

Параметр

Название **Система ESXi полностью обновлена**

Описание

Эталонное значение: **Обновления не требуются**

Обновлённая система ESXi может уменьшает возможность атаки. Злоумышленник может использовать известные уязвимости для того, чтобы получить доступ или повышение привилегий на хосте ESXi.

Исправление

Установите процесс, чтобы держать хосты ESXi в актуальном состоянии в соответствии с отраслевыми стандартами и внутренними инструкциями. VMware Update Manager представляет собой автоматизированное средство, которое может значительно помочь с этим. VMware публикует также Бюллетени безопасности и даёт возможность подписаться на оповещения по электронной почте. https://www.vmware.com/support/policies/security_response

Группа

Название **Виртуальные машины**

Описание

VirtualMachine - управляемый тип объекта для манипулирования виртуальными машинами, включающий шаблоны, которые могут быть развернуты (неоднократно) в качестве новых виртуальных машин. Этот тип обеспечивает способы конфигурирования и управления виртуальной машиной.

Если весь раздел "неприменим" - значит нет ни одной виртуальной машины на ESXi хосте.

Группа

Название **Отключить в явном виде операции копировать/вставить**

Описание

Копирование и вставка по умолчанию отключены. Тем не менее, если вы явно отключить эти функции аудита управления, то эти параметры вернут положительное значение.

Параметр

Название **Отключить операцию копирования**

Описание

Виртуальная машина должна быть максимально изолирована от ESXi хоста. *Эталонное значение:***True**

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.copy.disable" со значением "true".

Параметр

Название	**Отключить операцию перетаскивания**
Описание	

Эталонное значение: **True**

Виртуальная машина должна быть максимально изолирована от ESXi хоста.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.dnd.disable" со значением "true".

	Параметр
Название	**Отключить параметр setGUIOptions**
Описание	

Эталонное значение: **False**

Виртуальная машина должна быть максимально изолирована от ESXi хоста.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.setGUIOptions.enable" со значением "False".

	Параметр
Название	**Отключить операцию вставки**
Описание	

Эталонное значение: **True**

Виртуальная машина должна быть максимально изолирована от ESXi хоста.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.paste.disable" со значением "true".

	Группа
Название	**Отключить сжатие/очистку виртуального диска**
Описание	

Сжатие виртуального диска освобождает неиспользуемое пространство. Процесс сжатия уменьшает размер файлов диска на объем дискового пространства, восстановленного в процессе очистки. Если на диске есть пустое место, то этот процесс уменьшает объем пространства, занимаемого виртуальным диском, на основном диске. Обычные пользователи и процессы, то есть пользователи и процессы без привилегий root или администратора, имеют возможность вызвать эту процедуру на виртуальных машинах. Пользователь, не являющийся root, не может очистить части виртуального диска, требующие прав уровня root. Повторное сжатие диска может вызвать отказ в осбслуживании, так что следует отключить эту функцию.

	Параметр
Название	**Отключить сжатие виртуального диска**
Описание	

Эталонное значение: **True**

Отключить сжатие виртуального диска

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.diskShrink.disable" со значением "true".

Параметр	
Название	**Отключить очистку виртуального диска**
Описание	

Эталонное значение: **True**

Отключить очистку виртуального диска.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.diskWiper.disable" со значением "true".

Группа	
Название	**Отключить неэкспонированные функции**
Описание	

Некоторые параметры VMX не применимы к VMware vSphere, поскольку виртуальные машины VMware работают как на VMware vSphere так и на таких платформах виртуализации как Workstation и Fusion. Явное отключение неэкспонированных функций уменьшает вероятность уязвимости, поскольку уменьшается количество способов, которыми гость может повлиять на хост.

Параметр	
Название	**Отключить autologon**
Описание	

Эталонное значение: **True**

Явное отключение функции autologon уменьшает вероятность уязвимости. С автоматическим подключением вы можете сохранить учетные данные для входа и обойти диалоговое окно авторизации при включении питания на виртуальной машине Windows.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.ghi.autologon.disable" со значением "true".

Параметр	
Название	**Отключить biosbbs**
Описание	

Эталонное значение: **True**

Явное отключение функции BIOS Boot Specification (BBS) уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.bios.bbs.disable" со значением "true".

	Параметр
Название	**Отключить getcreds**
Описание	

Эталонное значение: **True**

Явное отключение функции getcreds уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.getCreds.disable" со значением "true".

	Параметр
Название	**Отключить launchmenu**
Описание	

Эталонное значение: **True**

Явное отключение функции launchmenu уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.ghi.launchmenu.change" со значением "true".

	Параметр
Название	**Отключить memsfss**
Описание	

Эталонное значение: **True**

Явное отключение функции memsfss уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.memSchedFakeSampleStats.disable" со значением "true".

	Параметр
Название	**Отключить protocolhandler**
Описание	

Эталонное значение: **True**

Явное отключение функции protocolhandler уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Разверните "Advanced Settings". Пролистайте список "Configuration Parameters" и убедитесь, что параметр "isolation.tools.ghi.protocolhandler.info.disable" существует и имеет значение "true".

Параметр	
Название	**Отключить shellaction**
Описание	

Эталонное значение: **True**

Явное отключение функции shellaction уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.ghi.host.shellAction.disable" со значением "true".

Параметр	
Название	**Отключить toporequest**
Описание	

Эталонное значение: **True**

Явное отключение функции toporequest уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.dispTopoRequest.disable" со значением "true".

Параметр	
Название	**Отключить trashfolderstate**
Описание	

Эталонное значение: **True**

Явное отключение функции trashfolderstate уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.trashFolderState.disable" со значением "true".

Параметр	
Название	**Отключить trayicon**
Описание	

Эталонное значение: **True**

Явное отключение функции trayicon уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.ghi.trayicon.disable" со значением "true".

Параметр	
Название	**Отключить unity**
Описание	

Эталонное значение: **True**

Явное отключение функции unity уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.unity.disable" со значением "true".

Параметр	
Название	**Отключить unity interlock**
Описание	

Эталонное значение: **True**

Явное отключение функции unity interlock уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.unityInterlockOperation.disable" со значением "true".

Параметр	
Название	**Отключить unitypush**
Описание	

Эталонное значение: **True**

Явное отключение функции unitypush уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.unity.push.update.disable" со значением "true".

Параметр	
Название	**Отключить unity taskbar**
Описание	

Эталонное значение: **True**

Явное отключение функции unity taskbar уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -

> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.unity.taskbar.disable" со значением "true".

Параметр	
Название	**Отключить unity unityactive**
Описание	

Эталонное значение: **True**

Явное отключение функции unity unityactive уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.unityActive.disable" со значением "true".

Параметр	
Название	**Отключить unity windowcontents**
Описание	

Эталонное значение: **True**

Явное отключение функции unity windowcontents уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.unity.windowContents.disable" со значением "true".

Параметр	
Название	**Отключить versionget**
Описание	

Эталонное значение: **True**

Явное отключение функции versionget уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.vmxDnDVersionGet.disable" со значением "true".

Параметр	
Название	**Отключить versionset**
Описание	

Эталонное значение: **True**

Явное отключение функции versionset уменьшает вероятность уязвимости.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -

> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.guestDnDVersionSet.disable" со значением "true".

Группа	
Название	**Отключить посторонние устройства**
Описание	

Например, последовательные и параллельные порты редко используются для виртуальных машин в центре обработки данных, а также CD/DVD диски, как правило, присоединяются временно во время установки программного обеспечения.

Параметр	
Название	**Отключить floppy устройства**
Описание	

Эталонное значение: **Не существует**

Убедитесь, что floppy устройства не подключены к виртуальной машине, если они не требуются.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Hardware". Нажмите "Edit". Удалите floppy устройства, если они существуют.

Параметр	
Название	**Отключить parallel устройства**
Описание	

Эталонное значение: **Не существует**

Убедитесь, что parallel устройства не подключены к виртуальной машине, если они не требуются. Например, последовательные и параллельные порты редко используются для виртуальных машин в центре обработки данных, а также CD / DVD диски, как правило, посоединяются временно во время установки программного обеспечения. Для менее часто используемых устройств, которые не требуются, параметр либо не должен присутствовать, либо его значение должно быть False. Когда значение False - функция отключена, однако устройство может по-прежнему отображаться в гостевой операционной системе.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Hardware". Нажмите "Edit". Удалите parallel устройства, если они существуют.

Параметр	
Название	**Отключить serial устройства**
Описание	

Эталонное значение: **Не существует**

Убедитесь, что serial устройства не подключены к виртуальной машине, если они не требуются.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Hardware". Нажмите "Edit". Remove serial устройства, если они существуют.

Группа

Название	**Предотвратить несанкционированное удаление, изменение устройства и подключение к нему**

Описание

В виртуальной машине пользователи и процессы без привилегий root или администратора могут подключать или отключать устройства такие как сетевые адаптеры и компакт-диски, а также могут изменять настройки устройств. С помощью виртуального редактора настроек машины или редактора конфигурации можно удалить ненужные или неиспользуемые аппаратные устройства. Необходимо запретить подключение, отключение и изменение устройства внутри гостевой операционной системы пользователям или запущенным процессам в виртуальной машине. По умолчанию, вредоносный пользователь с привилегиями nonadministrator в виртуальной машине имеет следующие полномочия:
1. Подключить отключенный привод CD-ROM и получить доступ к конфиденциальной информации СМИ, оставшийся в приводе
2. Отсоединить сетевой адаптер, чтобы изолировать виртуальную машину от сети, что является отказом в обслуживании
3. Измененить настройки устройства

	Параметр
Название	**Запретить несанкционированное подключение устройств**

Описание

Эталонное значение: **True**

Запретить несанкционированное подключение устройств для безопасности виртуальной машины.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.device.connectable.disable" со значением "true".

	Параметр
Название	**Запретить несанкционированное модификацию устройств**

Описание

Эталонное значение: **True**

Запретить несанкционированное изменение устройств для безопасности виртуальной машины.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.device.edit.disable" со значением "true".

	Параметр
Название	**Отключить передачу файлов HGFS**

Описание

Эталонное значение: **True**

Некоторые автоматизированные операции, например автоматическое обновление инструментов, используют компонент в гипервизоре под названием "Host Guest File System". Злоумышленник потенциально может использовать это для передачи файлов внутри гостевой ОС.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.hgfsServerSet.disable" со значением "true".

	Параметр
Название	**Отменить использование independent nonpersistent дисков**
Описание	

Эталонное значение: **Persistent/Independent_persistent**
Проблема безопасности с состоянием nonpersistent disk заключается в том, что злоумышленник с помощью простого выключения или перезагрузки может отменить или удалить любые следы с машины. Во избежание этого риска виртуальные машины должны быть в состоянии persistent disk; Кроме того, убедитесь, что активность в виртуальной машине логируется на удаленном сервере, таком как syslog server или эквивалентного коллектору событий на базе Windows. Без постоянного логирования виртуальной машины администраторы не узнают подвергалась ли она нападению или взлому.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Hardware". Нажмите "Edit". Разверните "Hard disk", перейдите в "Disk mode" и выберите "Independent - Nonpersistent".

	Параметр
Название	**Отключить VIX сообщения от виртуальной машины**
Описание	

Эталонное значение: **True**

VIX API это библиотека для написания скриптов и программ для управления виртуальными машинами. Если вы не используете пользовательское программирование VIX в вашей среде, то вам следует отключить определенные функции, чтобы уменьшить вероятность уязвимости. Возможность отправки сообщений из виртуальной машины на хост следует отключить. Обратите внимание, что отключение этой функции не влияет на функционирование операций VIX, которые возникают вне учётной записи гостя. Так что решения, которые используют VIX, будут работать.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.vixMessage.disable" со значением "true".

	Параметр
Название	**Отключить автоустановку**
Описание	

Эталонное значение: **True**

Инструменты автоматической установки может инициировать автоматическую перезагрузку.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "isolation.tools.autoInstall.disable" со значением "true".

	Параметр
Название	**Ограничить объём VMX файла с информационными сообщениями от виртуальной машины**
Описание	

Эталонное значение: **1048576**

Конфигурационный файл, содержащий пару имя-значение, ограничен размером 1 МБ. Этой емкости 1 МБ должно быть достаточно для большинства случаев, но вы можете увеличить это значение, если большое количество пользовательских данных хранятся в конфигурационном файле. Ограничение по умолчанию: 1 МБ, этот предел применяется даже в том случае, когда параметр SizeLimit не указан в файле .vmx. Неконтролируемый размер файла VMX может привести к отказу в обслуживании, если хранилище данных заполнено.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "tools.setInfo.sizeLimit" со значением "1048576".

	Параметр
Название	**Контролировать доступ к консоли виртуальной машины через VNC протокол**
Описание	

Эталонное значение: **False**

Консоль виртуальной машины позволяет подключиться, если монитор физического сервера подтвердит. Эта консоль также доступна по протоколу VNC. Настройка этого доступа также включает в себя создание правил брандмауэра для каждого ESXi сервера виртуальной машины.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "RemoteDisplay.vnc.enabled" со значением "False".

	Параметр
Название	**Отключить отправку информации о хосте гостю**
Описание	

Эталонное значение: **False**

Если параметр "tools.guestlib.enableHostInfo" имеет значение True, то виртуальная машина может получить подробную информацию о физическом хосте. Злоумышленник может использовать эту информацию для дальнейших атак на хост. Исключение составляет случаи, когда включение отправки информации о хосте необходимо для мониторинга производительности.
Значение по умолчанию для этого параметра - False, но оно отображается как Null. Установка False предназначена исключительно для целей аудита.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "tools.guestlib.enableHostInfo" со значением "False".

	Параметр
Название	**Проверить доступность виртуальной машины с присвоенной солью, которая совместно использует страницы памяти**
Описание	

Эталонное значение: **Site-Specific**

Когда соль включена (Mem.ShareForceSalting = 1 или 2), для того чтобы поделить страницу между двумя виртуальными машинами, соль и содержимое страницы памяти должны совпадать. Значение соли представляет собой настраиваемый параметр VMX для каждой виртуальной машины. Вы можете вручную указать значения соли в файле VMX виртуальной машины с новой опцией VMX sched.mem.pshare.salt. Если этот параметр не присутствует в файле VMX виртуальной машины, то берётся значение vc.uuid по умолчанию. Поскольку vc.uuid является уникальным для каждой виртуальной машины, то по умолчанию TPS встречается только среди страниц, принадлежащих к конкретной виртуальной машине (Intra-VM).
Если группа виртуальных машин считается надежной, то можно разделить страницы среди них, установив общее значение соли для всех этих виртуальных машин.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем измените "sched.mem.pshare.salt" на значение "Site-Specific".

	Параметр
Название	**Контролировать доступ к виртуальной машине через dvfilter network API**
Описание	

Эталонное значение: **Null**

Злоумышленник может поставить под угрозу безопасность виртуальной машины, используя dvFilter API.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "VM Options". Нажмите "Edit". Перейдите во вкладку "VM Options" и разверните "Advanced". Нажмите "Edit Configuration". Нажмите "Add Row" и затем добавьте параметр "ethernetn.filtern.name" parameter with the filtername value.

	Параметр
Название	**Контролировать использование функционала проброса PCI или PCIe**
Описание	

Эталонное значение: **NULL**

Использование функции VMware DirectPath I/O для проброса PCI или PCIe на виртуальную машину ведёт к потенциальной уязвимости в системе безопасности. Уязвимость может быть вызвана ошибочным или вредоносным кодом, запущенном в привилегированном режиме в гостевой ОС, например драйвером устройства. Стандартное оборудование и прошивка в настоящее время не имеют возможности закрыть эту уязвимость на ESXi.

Исправление

Из веб-клиента VMware vSphere выберите каждую виртуальную машину, нажмите "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Settings" -> "Virtual Hardware" -> Remove the PCI/PCIe passthrough device.

	Группа
Название	**vNetwork**
Описание	

Раздел представляет собой сетевые настройки как для хостов так и для виртуальных машин. Это может быть физической сеть или логическая сеть, такая как VLAN.

Если весь раздел "неприменим" - значит нет ни одного свитча.

	Параметр

Название	**Политика “Forged Transmits” отключена**

Описание

Эталонное значение: **Отключена**

Если операционная система виртуальной машины изменяет MAC адрес, то операционная система может передавать кадры с MAC-адресом отправителя в любое время. Это позволяет операционной системе создавать вредоносные атаки на устройствах в сети, выдавая себя за сетевой адаптер, разрешенный принимающей сетью.
Когда параметр "Forged Transmits" настроен "Accept", то ESXi не сравнивает источник и рабочие MAC-адреса.
Для защиты от подмены MAC-адреса вы можете настроить “Forged Transmits” на "Reject". В таком случае хост будет проверять на соответствие MAC-адрес отправителя, передаваемый от гостевой операционной системы, с рабочим MAC-адресом для своего виртуального адаптера. Если адреса не совпадают, то ESXi хост отбросит пакет.

Исправление

Из веб-клиента VMware vSphere ("Networking" -> "Virtual Switches" в 6.7) выберите хост и далее "Manage" ("Configure" в 6.5) -> "Networking" -> "Virtual Switches". Для каждого виртуального свитча и портгруппы в составе свитча нажмите edit. Во вкладке "Security" поменяйте политику "Forged transmits" на значение "Reject".

	Параметр
Название	**Политика “MAC Address Changes” отключена**

Описание

Эталонное значение: **Отключена**

Если операционная система виртуальной машины изменяет MAC адрес, то операционная система может передавать кадры с MAC-адресом отправителя в любое время. Это позволяет операционной системе создавать вредоносные атаки на устройствах в сети, выдавая себя за сетевой адаптер, разрешенный принимающей сетью.
Эта настройка позволит предотвратить изменение рабочего MAC-адреса в виртуальных машинах. Microsoft Clustering, например, требует от системы совместного использования MAC-адреса. Это также повлияет на работу layer 2 bridge; на приложения, которые требуют конкретного MAC-адреса для лицензирования. Исключение должно быть сделано для dvPortgroups, к которым подключены приложения.

Исправление

Из веб-клиента VMware vSphere ("Networking" -> "Virtual Switches" в 6.7) выберите хост и далее "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Networking" -> "Virtual Switches". Для каждого виртуального свитча и портгруппы в составе свитча нажмите edit. Во вкладке "Security" поменяйте политику "MAC address changes" на значение "Reject".

	Параметр
Название	**Политика “Promiscuous Mode” отключена**

Описание

Эталонное значение: **Отключена**

Когда “Promiscuous Mode” включен для dvPortgroup, все виртуальные машины, подключенные к dvPortgroup имеют возможность чтения всех пакетов по всей сети. “Promiscuous Mode” по умолчанию отключен на ESXi сервере - это и есть рекомендуемая настройка. Тем не менее, его можно включить для отладки, мониторинга и устранения неполадок. Может понадобиться возможность видеть все пакеты в VSWITCH. Исключение должно быть сделано для dvPortgroups, к которому эти приложения подключены, для того, чтобы обеспечить полную прозрачность трафика dvPortgroup.

Исправление

Из веб-клиента VMware vSphere ("Networking" -> "Virtual Switches" в 6.7) выберите хост и далее "Manage" ("Configure" в 6.5, "Edit" в 6.7) -> "Networking" -> "Virtual Switches". Для каждого виртуального свитча и портгруппы в составе свитча нажмите edit. Во вкладке "Security" поменяйте политику "Promiscuous Mode" policy to "Reject".

Конец отчета. RedCheck 2.6.3.2630.
RedCheckID: FA47DEEC-66D5-47E6-AB23-4086C4D1B994.