MaxPatrol VM версия 2.0

PDQL-запросы для анализа активов

Дата редакции документа: 07.07.2023

Содержание

1. Об этом документе

Этот справочник содержит информацию о стандартных запросах на языке PDQL, предназначенных для проверки конфигураций активов при работе в Positive Technologies MaxPatrol VM (далее также — MaxPatrol VM). В документе описаны наборы запросов и результаты применения этих запросов при анализе параметров различных систем.

Справочник адресован операторам, которые используют MaxPatrol VM для проверки корректности параметров информационных активов организации.

Комплект документации MaxPatrol VM включает в себя следующие документы:

- Этот документ.
- Руководство по внедрению — содержит информацию для внедрения продукта в инфраструктуре организации: от типовых схем развертывания до инструкций по установке, первоначальной настройке, обновлению и удалению продукта.
- Руководство администратора — содержит справочную информацию и инструкции по настройке и администрированию продукта.
- Руководство оператора — содержит сценарии использования продукта для управления информационными активами организации.
- Руководство по настройке источников — содержит рекомендации по интеграции элементов IT-инфраструктуры организации с MaxPatrol VM для аудита активов.
- Руководство разработчика — содержит информацию о доступных в MaxPatrol VM функциях сервиса REST API.
- Синтаксис языка запроса PDQL — содержит справочную информацию и примеры синтаксиса, основных функций и операторов языка PDQL, используемых при работе с MaxPatrol VM.

2. Запросы для Unix

Этот раздел содержит информацию о запросах на языке PDQL для работы с активами в ОС семейства Unix.

В этом разделе

2.1. Парольные политики

Количество сохраняемых паролей не соответствует требованиям

Если пользователь при очередной смене пароля укажет один из паролей, установленных ранее, злоумышленник сможет воспользоваться ранее скомпрометированным паролем. Вам нужно установить количество паролей, которые будут сохраняться в истории, в соответствии с политикой безопасности организации.

Количество сохраняемых паролей не должно быть меньше порогового значения.

Результат запроса: список систем, в которых заданное количество сохраняемых паролей меньше порогового значения.

Нестойкий алгоритм хеширования паролей

Если в системе используется нестойкий алгоритм хеширования паролей, локальный злоумышленник может быстро перебрать их. Вам нужно использовать стойкий алгоритм хеширования.

Результат запроса: список систем, в которых применяется нестойкий алгоритм хеширования паролей.

Недостаточная длина паролей

Отсутствие контроля за стойкостью паролей, которые назначают себе пользователи, может привести к успешной атаке методом перебора паролей со стороны как локального (при получении хеш-сумм), так и удаленного (словарные атаки через сетевые сервисы) злоумышленника. Вам нужно установить требование к минимальной длине пароля (рекомендуемое минимальное значение — 8 символов).

Результат запроса: список систем с недостаточными требованиями к длине пароля.

Недостаточное количество различных символьных классов в пароле

Отсутствие контроля за стойкостью паролей, которые назначают себе пользователи, может привести к успешной атаке методом перебора паролей со стороны как локального (при получении хеш-сумм), так и удаленного (словарные атаки через сетевые сервисы) злоумышленника. Вам нужно установить требование к минимальному количеству различных символьных классов, которые должны присутствовать в пароле (рекомендуемое минимальное количество классов — 3).

Результат запроса: список систем с недостаточными требованиями к количеству различных символьных классов в пароле.

Недостаточные требования к сроку действия паролей

Если вы не установите максимальное время действия пароля, у злоумышленника будет больше времени на то, чтобы подобрать пароль и использовать его для скрытого доступа к системе. Если вы не установите минимальное время действия пароля, пользователи смогут сменить несколько паролей подряд и установить тот пароль, который они использовали недавно, что повышает риск компрометации системы.

Результат запроса: список систем с недостаточными требованиями к сроку действия паролей.

2.2. Службы и сервисы

Автозапуск inetd

Подсистема inetd (xinetd) отвечает за запуск устаревших сетевых сервисов. Большинство из них открывает дополнительные векторы атаки для злоумышленника.

Результат запроса: список систем, на которых запущена подсистема inetd.

Автозапуск SMB и FTP

Рекомендуется отключить сервисы удаленного доступа FTP и SMB, если они не используются для критически важных задач. В противном случае при их неверной настройке (например, при возможности входа анонимного пользователя; при доступности всей файловой системы, а не изолированного окружения; при возможности изменения важных системных файлов) злоумышленник получит дополнительный удаленный вектор проникновения в систему.

Результат запроса: список систем, на которых запущены сервисы удаленного доступа SMB и (или) FTP.

Автозапуск R-сервисов

R-сервисы (сервисы удаленного доступа), такие как rlogin и rsh, позволяют удаленным пользователям входить в систему без указания пароля. Особенно опасными для R-сервисов являются тривиальные атаки ARP spoofing. Эти сервисы вам необходимо отключить. В настоящее время все программное обеспечение, которому они когда-то требовались (IBM NIM, HP Ignite-UX), поддерживает средства SSH, поэтому удаленные пользователи могут перейти на SSH и SCP.

Результат запроса: список систем с запущенными R-сервисами.

Разрешен удаленный вход без указания пароля с помощью rlogin или rsh

R-сервисы (сервисы удаленного доступа), такие как rlogin и rsh, позволяют удаленным пользователям входить в систему без указания пароля. Этим может воспользоваться злоумышленник.

Результат запроса: список систем, где разрешен удаленный вход без указания пароля в систему с помощью rlogin или rsh.

2.3. Настройка утилиты sudo

Разрешено выполнение любых команд от имени root

С помощью утилиты sudo администратор может предоставить пользователям право выполнять любые команды от имени суперпользователя (root) или других пользователей. Предоставление такого права всем пользователям является небезопасным.

Результат запроса: список систем, в которых пользователям разрешено выполнение любых команд от имени root.

Опасные команды

Неправильная настройка утилиты sudo может позволить пользователю выполнять потенциально опасные команды от имени суперпользователя (root). Такие команды могут позволить повышать привилегии в системе, а также перезаписывать системные файлы, нарушая тем самым работу системы.

Результат запроса: список систем, где разрешено выполнение команд, которые могут привести к компрометации системы.

2.4. Настройка загрузчиков

Не установлен пароль для доступа к настройке загрузчика FreeBSD

Если доступ к настройке загрузчика операционной системы FreeBSD не ограничен паролем, то этим может воспользоваться злоумышленник, получивший физический доступ к консоли сервера или средству управления виртуальными машинами. Он может перезагрузить сервер, в параметрах загрузчика BSD loader указать в качестве системы инициализации /bin/bash и получить тем самым доступ к системе с правами root (суперпользователя) без ввода пароля. Также злоумышленник может загрузить в ядро ОС свой модуль, который в дальнейшем будет исполняться с правами root.

Результат запроса: список систем, в которых не установлен пароль для доступа к настройке загрузчика FreeBSD.

Не установлен пароль для доступа к настройке загрузчика GRUB

Если доступ к настройке загрузчика GRUB не ограничен паролем, то этим может воспользоваться злоумышленник, получивший физический доступ к консоли сервера ОС или средству управления виртуальными машинами. Он может перезагрузить сервер, в параметрах загрузчика GRUB указать в качестве системы инициализации /bin/bash и получить тем самым доступ к операционной системе с правами root (суперпользователя) без ввода пароля. Также злоумышленник может загрузить в ядро ОС свой модуль, который в дальнейшем будет исполняться с правами root.

Результат запроса: список систем, в которых не установлен пароль для доступа к настройке загрузчика GRUB.

2.5. Права доступа

Некорректные права доступа к файлу с группами

При слабых правах доступа к файлам с описанием пользовательских групп (/etc/group) пользователи могут прочесть или перезаписать данные, добавить пользователей в группу администраторов, повысить свои права в системе.

Результат запроса: список систем с некорректными правами доступа к файлу с группами.

Некорректные права доступа к файлам с битами SUID или SGID

Файлы с установленным битом SUID выполняются с правами их владельца, файлы с установленным битом SGID — с правами группы владения, вне зависимости от того, кто запускает эти файлы. Если права доступа позволяют редактировать эти файлы любым пользователям, то злоумышленник сможет изменить их содержимое и выполнить произвольный код.

Результат запроса: список файлов с установленными битами SUID или SGID и некорректными правами доступа.

Некорректные права доступа к файлу с пользователями

При слабых правах доступа к файлу с описанием пользовательских идентификаторов (/etc/passwd) пользователи могут прочесть либо перезаписать хеш-суммы паролей, создать учетную запись с ролью администратора, повысить свои права в системе.

Результат запроса: список систем с некорректными правами доступа к файлу с пользователями.

Некорректные права доступа к сценариям, выполняющимся с помощью cron

С помощью cron могут вызываться как системные команды, так и различные пользовательские скрипты. Вам нужно предотвратить возможность изменения файлов, которые вызываются из заданий cron, неавторизованными пользователями. Иначе неавторизованные пользователи будут иметь возможность выполнять произвольный код от имени владельца задания cron (в том числе root, что приведет к полной компрометации системы).

Результат запроса: список систем с некорректными правами доступа к сценариям, выполняющимся с помощью cron.

Некорректные права доступа к стартовым сценариям

Все ОС семейства Unix осуществляют запуск сервисов при запуске ОС от имени суперпользователя (root) (вне зависимости от используемой подсистемы запуска — SysV init или upstart.systemd). Следовательно, если на исполняемые файлы сервисов (сценарии, бинарные файлы) установлены некорректные права доступа, локальный злоумышленник может изменить их содержимое и выполнить произвольный код с правами root при следующем запуске ОС или перезапуске сервиса.

Результат запроса: список систем с некорректными правами доступа к стартовым сценариям.

Некорректные права доступа к исполняемым файлам и библиотекам ОС

Все ОС семейства Unix запускают сервисы при запуске ОС от имени суперпользователя (root). Также во время работы ОС выполняется множество программ и сценариев от имени root. При некорректных правах доступа к исполняемым файлам и библиотекам ОС злоумышленник может изменить их содержимое и выполнить произвольный код с правами root при следующем запуске ОС или перезапуске сервиса.

Результат запроса: список систем с некорректными правами доступа к исполняемым файлам и библиотекам ОС.

Некорректные права доступа к файлам запущенных процессов

Права доступа к файлам запущенных процессов должны быть 755 или строже, их владельцами в подавляющем большинстве случаев должны являться суперпользователь (root) или системные пользователи (то есть пользователи, не имеющие возможности входить в систему с паролем). В противном случае непривилегированный пользователь может изменить содержимое файлов запущенных процессов, выполнить произвольный код с правами пользователя, запустившего процесс, и нарушить работоспособность системы.

Результат запроса: список систем с некорректными правами доступа к файлам запущенных процессов.

Пользователи с некорректными правами доступа к домашним каталогам

В домашних каталогах пользователей часто хранится информация, представляющая интерес для злоумышленника, например файлы журналов, история действий пользователей, различные архивы. Для домашних каталогов реальных (не виртуальных) пользователей вам нужно назначить права доступа, разрешающие чтение содержимого, модификацию и обращение к данным только самому пользователю.

Результат запроса: список пользователей с некорректными правами доступа к домашним каталогам.

2.6. Настройка пользователей

Пользователи с пустым паролем

Пользователи с пустым паролем представляют существенную угрозу для защиты целевой системы, так как в большинстве случаев злоумышленнику достаточно знать имя соответствующего пользователя для успешного удаленного входа в систему.

Результат запроса: список пользователей, для которых не указан пароль для входа в систему.

Пользователи с некорректным UID

Наличие иных пользователей, кроме суперпользователя (root), с UID, равным 0, может повлиять на производительность ОС, возможность отслеживания инцидентов, механизмы ограничения доступа (некоторые подсистемы защиты учитывают только UID, другие — только имя пользователя). Такая настройка ОС не требуется для решения прикладных задач, а в некоторых случаях свидетельствует об успешной компрометации системы, произошедшей ранее.

Результат запроса: список пользователей с UID, равным 0 (кроме root).

Пользователи с некорректными домашними каталогами

Вам нужно убедиться, что все интерактивные пользователи системы (то есть имеющие возможность входа в систему с исполнением команд) имеют свои отдельные домашние каталоги, отличные от корневого, и эти каталоги существуют. Так, например, во многих коммерческих ОС семейства Unix по традиции корневой каталог назначается для root как домашний. К корневому каталогу имеют доступ все пользователи. Соответственно, все файлы и каталоги, которые root создает у себя в $HOME, могут быть доступны для остальных пользователей как минимум для чтения.

Результат запроса: список интерактивных пользователей, у которых нет своих домашних каталогов, отличных от корневого.

2.7. Параметры журналирования

Не настроена отправка сообщений syslog на удаленный сервер

Отправка сообщений syslog на удаленный сервер позволяет долго хранить и анализировать данные о событиях, связанных с безопасностью. Вам нужно настроить отправку сообщений syslog на удаленный сервер.

Результат запроса: список систем, на которых не настроена отправка сообщений syslog на удаленный сервер.

3. Запросы для Oracle Database

Этот раздел содержит информацию о запросах на языке PDQL для работы с активами в СУБД Oracle Database.

В этом разделе

3.1. Параметры базы

Пользователям разрешена аутентификация на уровне ОС

Параметр `remote_os_authent` определяет, будет ли разрешено удаленным пользователям, прошедшим аутентификацию в операционной системе, подключаться к базе данных без проверки пароля. Многие системы SAP используют этот механизм (параметр `remote_os_authent` включен) для связи с базой данных Oracle: он обеспечивает анонимное удаленное соединение с базой данных, где хранятся все данные SAP. Если злоумышленник сможет определить, что для пользователя настроена аутентификация на уровне операционной системы, то у него появится возможность подключиться к учетной записи пользователя без предоставления учетных данных для аутентификации.

Результат запроса: список серверов, на которых разрешена аутентификация на уровне ОС.

Префикс аутентификации пользователей

Параметр `os_authent_prefix` указывает префикс, который Oracle Database использует для аутентификации пользователей, пытающихся подключиться к серверу. Oracle Database добавляет значение этого параметра к началу имени учетной записи пользователя. При запросе на соединение Oracle Database сравнивает имя пользователя с префиксом с именами пользователей Oracle Database в базе данных.

Результат запроса: список серверов, на которых Oracle Database использует для аутентификации пользователей префикс по умолчанию (`ops$`).

Использование внешних групп для управления БД

Параметр `os_roles` позволяет использовать внешние группы в управлении базой данных. Поскольку использование операционной системой внешних групп для управления базой данных может привести к перекрытию привилегий и снижению уровня безопасности, вам нужно настроить этот параметр в соответствии с требованиями вашей организации.

Результат запроса: список серверов, на которых пользователи могут использовать внешние группы ОС для управления базами данных.

Разрешена аутентификация с использованием файла паролей

Параметр `remote_login_passwordfile` определяет, будет ли Oracle Database использовать файл паролей для аутентификации пользователей в базе данных.

Использование файла паролей имеет следующие недостатки:

— не предусмотрена блокировка учетной записи;

— высокая уязвимость для атак подбора паролей;

— отсутствует парольная политика;

— любая учетная запись в данном файле имеет повышенные привилегии (SYSDBA, SYSOPER);

— хеш-суммы паролей хранятся в открытом виде.

Результат запроса: список серверов, на которых для аутентификации используется файл паролей.

Разрешено применять роли ОС удаленных пользователей

Параметр `remote_os_roles` позволяет применять роли ОС удаленных пользователей для управления базой данных. Использование ролей ОС удаленных пользователей для управления базой данных понижает уровень безопасности.

Результат запроса: список серверов, на которых разрешено применять роли ОС удаленных пользователей.

Нечувствительность пароля к регистру

Параметр `sec_case_sensitive_logon` определяет, будет ли учитываться регистр в паролях, используемых для входа в систему. Учет регистра в паролях в базе данных Oracle позволяет увеличить количество символов, которые могут использоваться в паролях, что минимизирует риск атак методом перебора.

Результат запроса: список серверов, на которых не учитывается регистр пароля.

Защита подключения к серверному процессу базы данных не соответствует требованиям

Параметр `sec_max_failed_login_attempts` устанавливает количество неудачных попыток подключения к серверному процессу базы данных, по достижении которого Oracle Database закрывает соединение. Если количество попыток подключения не ограничено, злоумышленник сможет успешно осуществить атаку методом перебора паролей или вызвать отказ систем. Вам нужно настроить этот параметр в соответствии с требованиями вашей организации (рекомендуемое значение — 10).

Результат запроса: список серверов, на которых количество неудачных попыток подключения к серверному процессу базы данных не ограничено.

3.2. Парольная политика

Отсутствует проверка сложности пароля

Параметр `password_verify_function` определяет функцию, которая будет использоваться для проверки надежности паролей. Такая проверка обеспечивает необходимый уровень стойкости: чувствительность пароля к регистру, запрет простых комбинаций, а также параметры изменений или истории пароля. Данный параметр не применяется к учетным записям, контролируемым файлом пароля Oracle.

Результат запроса: список серверов, на которых не используется функция проверки требований к паролю.

Неограниченное число неудачных попыток входа

Параметр `failed_login_attempts` задает количество неудачных попыток входа, после которых учетная запись блокируется (рекомендуемое значение — 5). Чем меньше у злоумышленника попыток подобрать пароль к учетным записям пользователей, тем ниже эффективность его атак.

Результат запроса: список серверов, на которых количество неудачных попыток входа не ограничено.

Срок истечения пароля проигнорирован

Параметр `password_grace_time` определяет количество дней после окончания срока действия пароля, по истечении которых учетная запись пользователя будет заблокирована. В течение этого дополнительного периода система будет предлагать пользователю сменить пароль каждый раз при попытке доступа к учетной записи (рекомендуемое значение — 3).

Результат запроса: список серверов, на которых дополнительный период для смены пароля не ограничен.

Срок действия пароля не ограничен

Параметр `password_life_time` определяет срок действия пароля, по истечении которого требуется его изменить (рекомендуемое значение — 90). При длительном использовании одних и тех же паролей возрастает риск успешного проведения атаки методом перебора.

Результат запроса: список серверов, на которых срок действия пароля не ограничен.

Разрешена автоматическая разблокировка учетной записи после блокировки

Параметр `password_lock_time` определяет количество дней, в течение которых учетная запись будет оставаться заблокированной после достижения максимально разрешенного количества неудачных попыток входа в систему.

Блокирование пользователя после нескольких неудачных попыток входа может предотвратить дальнейшее развитие атаки методом перебора паролей. Вам нужно настроить этот параметр в соответствии с требованиями вашей организации (рекомендуемое безопасное значение — UNLIMITED: в этом случае учетная запись никогда не будет разблокирована автоматически).

Результат запроса: список серверов, на которых возможна автоматическая разблокировка учетной записи.

Глубина парольной истории не соответствует требованиям

Параметр `password_reuse_max` определяет, сколько раз должна произойти смена пароля, прежде чем пароль можно будет использовать повторно (рекомендуемое значение — 10). Повторное использование пароля через короткий промежуток времени снижает уровень защищенности.

Результат запроса: список серверов, на которых количество новых паролей, по истечении которых можно использовать старые пароли, не соответствует требованиям.

Количество дней, по истечении которых возможно повторное использование пароля, не соответствует требованиям

Параметр `password_reuse_time` определяет количество дней, которое должно пройти, прежде чем пароль можно будет использовать повторно (рекомендуемое значение — 180). Повторное использование пароля через короткий промежуток времени снижает уровень защищенности системы.

Результат запроса: список серверов, на которых количество дней, по истечении которых можно повторно использовать старые пароли, не соответствует требованиям.

3.3. Учетные записи и права доступа

Демонстрационные данные

Демонстрационные схемы Oracle Database включают в себя информацию, имеющую отношение к простым схемам, например относящимся к средствам управления персоналом (human resources), бизнес-аналитики (business intelligence), коллективного пользования (order entry). Эти схемы содержат набор демонстрационных данных: учетные записи пользователей (BI, HR, OE, PM, IX, SH, SCOTT), а также таблицы и фиктивные данные. Демонстрационные данные обычно не требуются для проведения производственных операций в базе данных. Они предоставляют пользователям хорошо известные стандартные пароли, конкретные представления и процедуры или функции. Такие учетные записи пользователей, представления, процедуры или функции могут быть использованы злоумышленниками для запуска средств эксплуатации уязвимостей рабочих сред.

Результат запроса: список серверов, на которых присутствуют демонстрационные данные.

Предоставлен доступ к таблице SYS.AUD$

Таблица аудита SYS.AUD$ базы данных Oracle содержит записи обо всех действиях, выполненных в базе данных (неудачные попытки действий также записываются в эту таблицу). Если рядовые пользователи имеют права на управление таблицей аудита SYS.AUD$, возрастает риск искажения записей аудита и скрытия несанкционированных действий. В целях безопасности рекомендуется разрешить доступ к таблице SYS.AUD$ только пользователям с привилегиями SYS, SYSTEM, а также пользователям, которым назначена роль DBA.

Результат запроса: список серверов, на которых существуют пользователи с правами на управление таблицей SYS.AUD$ (не учитываются пользователи с привилегиями SYS, SYSTEM и ролью DBA).

Предоставлен доступ к таблице SYS.LINK$

Таблица базы данных Oracle SYS.LINK$ содержит всю информацию о связях между базами, включая логины и хеш-суммы паролей. Если рядовые пользователи имеют права на управление таблицей SYS.LINK$ или просматривать ее, возрастает риск перехвата данных о паролях и повреждения основных связей базы данных. В целях безопасности рекомендуется разрешить доступ к таблице SYS.LINK$ только пользователям с привилегиями SYS, SYSTEM, а также пользователям, которым назначена роль DBA.

Результат запроса: список серверов, на которых существуют пользователи с правами на управление таблицей SYS.LINK$ (не учитываются пользователи с привилегиями SYS, SYSTEM и ролью DBA).

Предоставлен доступ к таблице SYS.SOURCE$

В таблице SYS.SOURCE$ хранятся исходные коды всех объектов базы данных. Имея доступ к исходному коду, злоумышленник может повысить свои привилегии до администратора базы данных и вывести базу данных из строя. В целях безопасности рекомендуется разрешить доступ к таблице SYS.SOURCE$ только пользователям с привилегиями SYS, SYSTEM, а также пользователям, которым назначена роль DBA.

Результат запроса: список серверов, на которых существуют пользователи с правами управления таблицей SYS.SOURCE$ (не учитываются пользователи с привилегиями SYS, SYSTEM и ролью DBA).

Предоставлен доступ к таблице SYS.USER_HISTORY$

Таблица базы данных Oracle SYS.USER_HISTORY$ содержит историю изменений паролей пользователей. Если злоумышленник прочтет хеш-суммы паролей пользователей базы данных, то сможет провести атаку методом перебора паролей. В целях безопасности рекомендуется разрешить доступ к таблице SYS.USER_HISTORY$ только пользователям с привилегиями SYS, SYSTEM, а также пользователям, которым назначена роль DBA.

Результат запроса: список серверов, на которых существуют пользователи с правами управления таблицей SYS.USER_HISTORY (не учитываются пользователи с привилегиями SYS, SYSTEM и ролью DBA).

Предоставлен доступ к таблице SYS.USER$

Таблица базы данных Oracle SYS.USER$ содержит хеш-суммы паролей пользователей. Если злоумышленник получит к ней доступ, то сможет запустить атаку методом перебора паролей. В целях безопасности рекомендуется разрешить доступ к таблице SYS.USER$ только пользователям с привилегиями SYS, SYSTEM, а также пользователям, которым назначена роль DBA.

Результат запроса: список серверов, на которых существуют пользователи с правами управления таблицей SYS.USER$ (не учитываются пользователи с привилегиями SYS, SYSTEM и ролью DBA).

4. Запросы для Windows

Этот раздел содержит информацию о запросах на языке PDQL для работы с активами в ОС семейства Windows.

В этом разделе

4.1. Контроль учетных записей (UAC)

Установка ПО без уведомления пользователей

Параметр определяет, каким образом Windows реагирует на запросы установки приложений. Этот параметр гарантирует, что пользователи и администраторы будут знать об установке нового программного обеспечения и должны будут в явной форме разрешить установку. Осведомленность о процессах установки программного обеспечения позволит вам избежать риска непреднамеренной установки несанкционированного ПО.

Результат запроса: активы, на которые можно устанавливать программное обеспечение, не уведомляя об этом пользователей.

Выключен контроль учетных записей (UAC)

Параметр позволяет повысить осведомленность о процессах, происходящих в системе. Использование данного параметра позволит вам избежать ситуации, когда в систему вносят изменения без вашего ведома.

Результат запроса: активы, на которых выключен контроль учетных записей пользователей (UAC).

4.2. Программы и службы

Путь службы содержит пробелы и не взят в кавычки

Службы могут быть использованы злоумышленником для запуска небезопасных программ с повышенными привилегиями. Когда путь службы содержит пробелы и не взят в кавычки, он может быть использован для подмены пути до исполняемого файла. Например, в службе

указан путь (C:\Program Files (x86)\Common Files\Microsoft Shared\Source Engine\OSE.EXE), который не взят в кавычки и запускается от имени администратора системы. Злоумышленник может изменить путь (C:\Program.exe) и запустить свою программу с повышенными привилегиями.

Результат запроса: активы, на которых пути служб содержат пробелы и не взяты в кавычки.

Установка ПО с повышенными привилегиями

Установщик Microsoft Windows может выполнять установку всех программ с повышенными привилегиями. Если этот параметр отключен, система при установке программ применяет права текущего пользователя, которые могут отличаться от прав системного администратора. Включение этого параметра может позволить всем пользователям устанавливать любые программы с правами администратора, что повышает риск установки потенциально небезопасного программного обеспечения.

Результат запроса: активы, на которые пользователям разрешено устанавливать программное обеспечение используя повышенные привилегии.

4.3. Параметры автозапуска

Разрешен автозапуск устройств, не являющихся томами

Этот параметр запрещает автозапуск устройств MTP, например фотокамер и телефонов. Злоумышленник может использовать автозапуск, чтобы нанести вред компьютеру или хранящимся на нем данным.

Результат запроса: активы, на которых разрешен автозапуск устройств, не являющихся томами.

Разрешен автозапуск при подключении съемных носителей

Этот параметр определяет, разрешен ли автозапуск. Автозапуск отключен по умолчанию на некоторых типах съемных дисков (например, на дискетах или сетевых дисках, но не на компакт-дисках). Вам нужно отключать автозапуск для всех типов съемных дисков: это уменьшит вероятность непреднамеренного запуска потенциально небезопасного приложения при подключении съемных носителей.

Результат запроса: активы, на которых разрешен автозапуск при подключении съемных носителей.

4.4. Параметры для анонимных аккаунтов

Трансляция анонимного SID в имя

Анонимный пользователь может получить имя учетной записи, зная идентификатор безопасности (security identifier, SID). Если анонимному пользователю разрешено получать имя аккаунта по SID, это может быть использовано злоумышленником для раскрытия имен пользователей, например настоящего имени администратора.

Результат запроса: активы, у которых анонимный SID транслируется в имя учетной записи пользователей.

Анонимный доступ к общим сетевым ресурсам

Анонимный пользователь может получить доступ к общим сетевым ресурсам. Это может быть использовано для подготовки проведения атак и для сбора конфиденциальной информации.

Результат запроса: активы, имеющие анонимный доступ к общим сетевым ресурсам.

Анонимный доступ к именованным каналам

Данный параметр содержит информацию об именованных каналах, к которым анонимный пользователь имеет доступ. Эта информация может быть использована для подготовки проведения атак и для сбора конфиденциальной информации.

Результат запроса: активы, имеющие анонимный доступ к именованным каналам.

4.5. Небезопасный уровень проверки подлинности LAN Manager

Параметр определяет, каким протоколом будет пользоваться система для аутентификации. Небезопасным считается любой параметр, кроме параметра **Отправлять только NTLMv2 ответ, отказывать LM и NTLM** (`Send NTLMv2 response only\refuse LM & NTLM`).

Результат запроса: активы, у которых небезопасный уровень проверки подлинности LAN Manager.

4.6. Парольные политики

Глубина парольной истории не соответствует требованиям

Рекомендуемая политика паролей требует, чтобы пользователи регулярно меняли пароли, а также чтобы текущий пароль отличался от тех паролей, которые хранятся в кэше.
Параметр определяет, сколько предыдущих паролей будет храниться, чтобы гарантировать, что пользователи не используют один набор паролей постоянно.

Результат запроса: активы, на которых количество новых паролей, по истечении которых можно использовать старые пароли, не соответствует требованиям.

Минимальная длина пароля не соответствует требованиям

Отсутствие контроля за стойкостью паролей, которые назначают себе пользователи, может привести к успешной атаке перебора паролей со стороны как локального (при получении хеш-сумм), так и удаленного (словарные атаки через сетевые сервисы) злоумышленника. Вам нужно задать требования к стойкости паролей, включающие в себя минимальную длину и количество различных символов в пароле.

Результат запроса: активы, на которых минимально допустимая длина пароля меньше порогового значения.

Минимальная длина пароля для рабочих станций не соответствует требованиям

Результат запроса: рабочие станции, на которых минимально допустимая длина пароля меньше порогового значения — 8.

Минимальная длина пароля для серверов не соответствует требованиям

Результат запроса: серверы, на которых минимально допустимая длина пароля меньше порогового значения — 14.

Срок действия пароля для рабочих станций не соответствует требованиям

Если не установить минимальное время действия пароля, пользователи могут сменить несколько паролей подряд и установить тот пароль, который они использовали недавно, что повышает риск компрометации системы. Если не установить максимальное время действия пароля, у злоумышленника будет больше времени на то, чтобы подобрать пароль и использовать его для скрытого доступа к инфраструктуре.

Результат запроса: рабочие станции, на которых минимально допустимый срок действия пароля меньше порогового значения — 1 и (или) максимально допустимый срок действия пароля больше порогового значения — 60.

Срок действия пароля для серверов не соответствует требованиям

Если не установить минимальное время действия пароля, пользователи могут сменить несколько паролей подряд и установить тот пароль, который они использовали недавно, что повышает риск компрометации системы. Если не установить максимальное время действия пароля, у злоумышленника будет больше времени на то, чтобы подобрать пароль и использовать его для скрытого доступа к инфраструктуре.

Результат запроса: серверы, на которых минимально допустимый срок действия пароля меньше порогового значения — 1 и (или) на которых максимально допустимый срок действия пароля больше порогового значения — 30.

Не требуется пароль при выходе из спящего режима

Параметр обязывает пользователя вводить пароль при выходе из спящего режима. Это сокращает вероятность неавторизованного доступа к системе.

Результат запроса: активы, на которых не требуется пароль при выходе из спящего режима.

Вход в систему без пароля

Параметр определяет, может ли пользователь, имеющий физический доступ к компьютеру, автоматически входить в систему. Этот параметр позволяет ограничить доступ к компьютеру и сетям, к которым он подключен, для неавторизованных пользователей, имеющих физический доступ к компьютеру и сетям.

Результат запроса: активы, на которых не требуется пароль при входе в систему.

5. Запросы для сетевых устройств

Этот раздел содержит информацию о запросах на языке PDQL для работы с сетевыми устройствами.

Входными данными для проверок на соответствие требованиям служат результаты аудита сетевых устройств. Для аудита вам нужно использовать протокол SSH, поскольку другие протоколы (такие как SNMP, Check Point OPSEC CPMI) не приносят необходимых для проверок данных в достаточном объеме.

В этом разделе

5.1. Маршрутизаторы

Все проверки применяются к сетевым устройствам, на которых включена маршрутизация IPv4 и (или) IPv6. Если маршрутизация отключена, устройство исключается из проверки.

В этом разделе

5.1.1. Защита контрольного и передающего уровней

Направленная широковещательная передача

Направленная широковещательная передача позволяет отправить широковещательный IP-пакет в удаленную сеть. По прибытии пакета в удаленную сеть передающее устройство рассылает пакет как широковещательный кадр канального уровня всем станциям в сети. Эта функциональность используется в качестве средства усиления и отражения в ряде атак. Вам нужно отключить направленную широковещательную передачу на всех интерфейсах.

Результат запроса: интерфейсы, на которых включена направленная широковещательная передача.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Eltex MES (ROS), Juniper Junos OS.

Proxy ARP

Proxy ARP — техника, при которой одно устройство, обычно маршрутизатор, отвечает на ARP-запросы, предназначенные другому устройству. Представляясь другим устройством, маршрутизатор берет на себя доставку пакетов реальной точке назначения. Использование Proxy ARP может привести к увеличению ARP-трафика в сетевом сегменте, истощению ресурсов и атакам типа «человек посередине». Вам нужно отключить Proxy ARP на всех интерфейсах.

Результат запроса: интерфейсы, на которых включен Proxy ARP.

Поддерживаемые системы: Alcatel AOS, Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Huawei VRP, Juniper Junos OS, Qtech NOS.

ICMP redirect

Сообщение ICMP redirect может быть сгенерировано маршрутизатором, когда пакет получен и отправлен на одном и том же интерфейсе. Злоумышленник может эксплуатировать способность маршрутизатора отправлять сообщения ICMP redirect, постоянно отправляя пакеты маршрутизатору, вынужденному отвечать сообщениями ICMP redirect, что негативно сказывается на загрузке центрального процессора и производительности маршрутизатора. Вам нужно отключить отправку сообщений ICMP redirect на всех интерфейсах.

Результат запроса: интерфейсы и семейства адресов, для которых включена отправка ICMP-сообщений о перенаправлении.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Eltex ESR, Eltex MES (ROS), Juniper Junos OS.

> **Примечание.** Некоторые системы (такие как Juniper Junos OS) предоставляют возможность глобального отключения функциональности ICMP redirect. Это не влияет на результат запроса, который проверяет только параметры интерфейсов.

ICMP unreachable

Фильтрация трафика списком доступа на интерфейсе вызывает отправку сообщений ICMP unreachable источнику трафика. Генерация таких сообщений может вызвать повышенную загрузку центрального процессора устройства. Вам нужно отключить отправку сообщений ICMP unreachable на всех интерфейсах.

Результат запроса: интерфейсы и семейства адресов, для которых включена отправка ICMP-сообщений о недостижимости.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Eltex ESR, Eltex MES (ROS).

> **Примечание.** Для некоторых ОС, например для Juniper Junos OS, отправка сообщений ICMP unreachable или отказ от нее определяется действием, указанным в правиле политики безопасности. Для таких систем проверка на интерфейсах неприменима.

Маршрутизация от исходного адреса

Маршрутизация от исходного IP-адреса использует параметры IP-пакета Loose Source Route или Strict Source Route вместе с параметром Record Route для того, чтобы позволить источнику IP-пакета указать путь, по которому должен пройти пакет. Эта функциональность может быть использована в попытках маршрутизации трафика в обход средств контроля безопасности. Вам нужно отключить маршрутизацию от исходного адреса.

Результат запроса: устройства, на которых включена маршрутизация от исходного адреса.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE.

Отключена одноадресная пересылка по обратному пути (uRPF)

Злоумышленники часто используют подмену IP-адресов источника для достижения цели атаки или для скрытия истинного источника атаки и воспрепятствования отслеживанию. Одноадресная пересылка по обратному пути (uRPF) позволяет устройству удостовериться, что адрес источника пакета может быть доступен через интерфейс, на котором получен пакет. Вам нужно включить uRPF на всех интерфейсах.

Результат запроса: интерфейсы и семейства адресов, для которых отключена одноадресная пересылка по обратному пути.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Huawei VRP, Juniper Junos OS.

5.1.2. Протоколы отказоустойчивости шлюза по умолчанию (FHRP)

Аутентификация FHRP не соответствует требованиям

Неаутентифицированная коммуникация при использовании протоколов отказоустойчивости шлюза по умолчанию позволяет атакующему выступить в роли шлюза по умолчанию в сетевом сегменте, что позволяет выполнить атаку типа «человек посередине» и перехватить весь пользовательский трафик, исходящий из сети. Вам нужно настроить аутентификацию FHRP с использованием максимально безопасного метода, поддерживаемого конкретным устройством для конкретной версии протокола.

Результат запроса: интерфейсы, на которых аутентификация протоколов отказоустойчивости шлюза по умолчанию не соответствует требованиям.

Таблица 1. Поддерживаемые системы и протоколы

ОС	Протокол	Версия	Требуемые методы аутентификации	Недопустимые методы аутентификации
Check Point GAiA	VRRP	2	simple	none
Cisco IOS	HSRP	1, 2	md5	simple, none
	VRRP	2	md5	simple, none
Cisco IOS XE	HSRP	1, 2	md5	simple, none
	VRRP	2	simple	none
Cisco IOS XR	HSRP	Нет данных[1]	simple	none
	VRRP		simple	none
Check Point GAiA	VRRP	2	simple	none
Cisco IOS	HSRP	1, 2	md5	simple, none
	VRRP	2	md5	simple, none
Cisco NX-OS	HSRP	1	simple	none
		2	md5	simple, none
	VRRP	Нет данных[1]	simple	none
HP Comware	VRRP		md5	simple, none
Huawei VRP	VRRP		md5	simple, none
Juniper Junos OS	VRRP	2	md5	simple, none

Версия 3 протокола VRRP не поддерживает аутентификацию и по этой причине не подпадает под проверку. VRRP для IPv6 поддерживается только в версии 3.

См. также

1

1 Указанные системы не выводят информацию о версии VRRP для IPv4.

5.1.3. Протоколы маршрутизации

Отсутствие аутентификации при обмене маршрутной информацией позволяет злоумышленнику внедрить ложную маршрутную информацию в сеть. При использовании криптографической аутентификации содержимое маршрутного обновления более устойчиво к попыткам подделки. Вам нужно настроить аутентификацию протоколов маршрутизации с использованием максимально безопасного метода, поддерживаемого конкретным устройством для конкретной версии протокола.

BGP: соседи без аутентификации

Результат запроса: соседи BGP, для которых не задан ключ аутентификации или связка ключей.

Поддерживаемые системы: Alcatel AOS, Check Point GAiA, Cisco IOS, Cisco IOS XE, Huawei VRP, Juniper Junos OS.

> **Примечание.** Системы Cisco ASA и Cisco NX-OS не поддерживают аутентификацию BGP, для них проверка неприменима.

OSPF: аутентификация областей не соответствует требованиям

Результат запроса: области OSPF, для которых аутентификация не задана или задан открытый пароль.

Поддерживаемые системы: Cisco ASA, Cisco IOS, Cisco IOS XE, Cisco NX-OS, Huawei VRP.

> **Примечание.** Системы Alcatel AOS, Check Point GAiA и Juniper Junos OS не поддерживают задание аутентификации OSPF на уровне областей, поэтому для них проверка неприменима.

OSPF: аутентификация интерфейсов не соответствует требованиям

Результат запроса: интерфейсы OSPF, для которых аутентификация не задана или задан открытый пароль.

Поддерживаемые системы: Alcatel AOS, Check Point GAiA, Cisco ASA, Cisco IOS, Cisco IOS XE, Cisco NX-OS, Huawei VRP, Juniper Junos OS.

OSPF: аутентификация виртуальных каналов не соответствует требованиям

Результат запроса: виртуальные каналы OSPF, для которых аутентификация не задана или задан открытый пароль.

Поддерживаемые системы: Alcatel AOS, Check Point GAiA, Cisco IOS, Cisco IOS XE, Cisco NX-OS, Huawei VRP, Juniper Junos OS.

Примечание. На Cisco ASA вы можете настроить аутентификацию виртуальных каналов, но она не будет влиять на обмен маршрутной информацией из-за дефекта производителя (Cisco bug CSCtb30476, подробнее см. на сайте cisco.com). Вместо настройки аутентификации виртуальных каналов производитель рекомендует использовать аутентификацию на интерфейсах. По этой причине данная проверка не применяется на Cisco ASA.

RIP: аутентификация интерфейсов не соответствует требованиям

Результат запроса: интерфейсы RIP, для которых аутентификация не задана или задан открытый пароль.

Поддерживаемые системы: Alcatel AOS, Check Point GAiA, Cisco ASA, Cisco IOS, Cisco IOS XE, Cisco NX-OS, Huawei VRP, Juniper Junos OS.

EIGRP: интерфейсы без аутентификации

Результат запроса: интерфейсы EIGRP, для которых не задана аутентификация.

Поддерживаемые системы: Cisco ASA, Cisco IOS, Cisco IOS XE, Cisco NX-OS.

5.2. Коммутаторы

Проверки применяются к сетевым устройствам — коммутаторам. Критерием проверки является наличие у устройства таблицы MAC-адресов. Устройство может выполнять роли маршрутизатора и коммутатора одновременно. В таком случае к нему будут применены проверки из обеих групп. В интерфейсе MaxPatrol VM такое устройство будет отображаться со значком маршрутизатора.

Защита портов не включена (проверка по умолчанию)

Защита портов используется против подмены MAC-адресов на интерфейсе доступа. Вам необходимо включить защиту портов на всех интерфейсах доступа.

Результат запроса: интерфейсы доступа, на которых не включена защита портов.

Поддерживаемые системы: Alcatel AOS, Cisco NX-OS, Huawei VRP, Juniper Junos OS.

Примечание. Поддерживается только классическая настройка защиты портов на уровне интерфейса. Варианты параметров защиты портов, встречающиеся только на Juniper Junos OS (параметры, общие для всех интерфейсов (interface all), и параметры, специфичные для конкретных VLAN), не анализируются и не проверяются.

Защита портов не включена (Cisco IOS)

Защита портов используется против подмены MAC-адресов на интерфейсе доступа. Вам необходимо включить защиту портов на всех интерфейсах доступа.

Результат запроса: интерфейсы доступа, на которых не включена защита портов.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE.

> **Примечание.** Проверка для Cisco IOS отличается из-за поддержки DTP. Под портами доступа понимаются только интерфейсы, сконфигурированные в режиме статического доступа. Динамические порты (независимо от их фактического состояния) не проверяются.

Отключен DHCP snooping

DHCP snooping обеспечивает сетевую безопасность путем фильтрации недоверенных DHCP-сообщений и построения таблицы привязок адресов. DHCP snooping позволяет различать недоверенные интерфейсы, к которым подключены конечные пользователи, и доверенные интерфейсы, подключенные к DHCP-серверу или другому коммутатору. Вам нужно включить DHCP snooping глобально и во всех VLAN.

Результат запроса: коммутаторы, на которых DHCP snooping отключен глобально.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco NX-OS, Huawei VRP.

> **Примечание.** Статус DHCP snooping для отдельных VLAN не проверяется.

5.3. Защита уровня управления устройством

Этот раздел содержит информацию о параметрах защиты уровня управления устройством.

В этом разделе

5.3.1. Небезопасные протоколы управления

Протокол Telnet передает трафик сеанса управления в открытом виде. Злоумышленник может получить доступ к конфиденциальной информации об устройстве и о сети. Вам нужно отключить доступ к устройству по Telnet.

Доступ по протоколу Telnet (проверка по умолчанию)

Результат запроса: устройства, на которых включена служба Telnet.

Поддерживаемые системы: Check Point GAiA, Cisco NX-OS, Cisco WLC (AireOS), Eltex ESR, Eltex MES (ROS), Juniper Junos OS, Avaya (Nortel) NNOS.

Доступ по протоколу Telnet (Cisco IOS)

Результат запроса: линии управления, на которых включен доступ по протоколу Telnet.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE.

Доступ по протоколу Telnet (Cisco ASA)

Результат запроса: устройства Cisco ASA, на которых разрешен доступ по протоколу Telnet, а также адреса и интерфейсы, с которых открыт доступ.

Поддерживаемые системы: Cisco ASA.

> **Примечание.** Доступ к устройству Cisco ASA по Telnet закрыт, если в конфигурации отсутствуют адреса, с которых доступ разрешен явно командой telnet.

Доступ по протоколу HTTP

Протокол HTTP передает трафик сеанса управления в открытом виде. Злоумышленник может получить доступ к конфиденциальной информации об устройстве и о сети. Вам нужно отключить доступ к устройству по HTTP.

Результат запроса: устройства, на которых включено управление по протоколу HTTP.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco NX-OS, Cisco WLC (AireOS), Juniper Junos OS, Avaya (Nortel) NNOS.

> **Примечание.** На устройствах Check Point (GAiA и SecurePlatform), Cisco ASA, Fortinet FortiOS веб-интерфейс управления доступен только по HTTPS.

Доступ по протоколу TFTP (Cisco IOS)

Протокол TFTP передает данные без аутентификации и в открытом виде. Злоумышленник может получить доступ к конфиденциальной информации об устройстве и о сети. Вам нужно отключить службу TFTP.

Результат запроса: устройства Cisco IOS, на которых включена служба TFTP.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE.

Доступ по протоколу SSH версии 1

Версия 1 протокола SSH считается небезопасной, поскольку содержит множество уязвимостей. Успешная атака позволит злоумышленнику, например, удаленно подключиться к устройству и выполнить произвольные команды или вызвать отказ в обслуживании.

Результат запроса: сетевые устройства, на которых включено управление по протоколу SSH версии 1.

Поддерживаемые системы: Cisco ASA, Cisco IOS, Cisco IOS XE, Cisco IOS XR, Eltex ESR, Huawei VRP, Juniper Junos OS, Avaya (Nortel) NNOS.

> **Примечание.** На устройствах Check Point (GAiA и SecurePlatform) доступна только версия 2 протокола SSH.

5.3.2. Списки доступа

Списки доступа контролируют, с каких адресов возможны попытки входа для управления устройством. Вам нужно настроить списки доступа или аналогичные ограничения для протоколов управления устройством.

Не заданы списки доступа для IOS и VRP (IPv4)

Запрос находит все устройства Cisco IOS и Huawei VRP, на которых хотя бы для одной из линий управления vty не задан список доступа для IPv4 во входящем направлении. В таблицу выводится информация обо всех линиях управления vty на таких устройствах и обо всех настроенных на них списках доступа во всех направлениях для всех семейств адресов, для того чтобы обеспечить полный контекст для поиска недостающих параметров. Вы можете использовать этот запрос, если в сети отсутствует адресация IPv6 и достаточно ограничить доступ по IPv4.

Результат запроса: устройства Cisco IOS и Huawei VRP, на которых не указаны списки доступа на линиях управления для протокола IPv4.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Huawei VRP.

Не заданы списки доступа для IOS и VRP (IPv4 и IPv6)

Запрос находит все устройства Cisco IOS и Huawei VRP, на которых хотя бы для одной из линий управления vty не заданы списки доступа для IPv4 и для IPv6 во входящем направлении. В таблицу выводится информация обо всех линиях управления vty на таких устройствах и обо всех настроенных на них списках доступа во всех направлениях для всех семейств адресов, для того чтобы обеспечить полный контекст для поиска недостающих параметров. Вы можете использовать этот запрос, если на интерфейсах сетевых устройств присутствуют адреса IPv6. Вне зависимости от того, маршрутизируются ли они за пределы локального сегмента, необходимо ограничить доступ для обоих семейств адресов.

Результат запроса: устройства Cisco IOS и Huawei VRP, на которых не указаны списки доступа на линиях управления для протокола IPv4 и (или) IPv6.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Huawei VRP.

Не заданы списки доступа для NX-OS (IPv4)

Для NX-OS существует два способа ограничения доступа к уровню управления устройством — применение списков доступа к линии управления vty и к управляющему интерфейсу mgmt0 (для Nexus 1000V только последний). Запрос находит все устройства Cisco Nexus, на которых список доступа для IPv4 не назначен во входящем направлении ни на линию vty, ни на интерфейс mgmt0. Для таких устройств в таблицу выводится информация обо всех списках доступа, назначенных во всех направлениях для всех семейств адресов — как на линию vty, так и на интерфейс mgmt0. Это необходимо для того, чтобы обеспечить полный контекст для поиска недостающих параметров. Вы можете использовать этот запрос, если в сети отсутствует адресация IPv6 и достаточно ограничить доступ по IPv4.

Результат запроса: устройства Cisco Nexus, на которых не указаны списки доступа для протокола IPv4.

Поддерживаемые системы: Cisco NX-OS.

> **Примечание.** Для одного и того же устройства информация о линии vty и об интерфейсе mgmt0 выводится в разных строках таблицы.

Не заданы списки доступа для NX-OS (IPv4 и IPv6)

Для NX-OS существует два способа ограничения доступа к уровню управления устройством — применение списков доступа к линии управления vty и к управляющему интерфейсу mgmt0 (для Nexus 1000V только последний). Запрос находит все устройства Cisco Nexus, на которых списки доступа для IPv4 и для IPv6 не назначены во входящем направлении ни на линию vty, ни на интерфейс mgmt0. Для таких устройств в таблицу выводится информация обо всех списках доступа, назначенных во всех направлениях для всех семейств адресов — как на линию vty, так и на интерфейс mgmt0. Это необходимо для того, чтобы обеспечить полный контекст для поиска недостающих параметров. Вы можете использовать этот запрос, если на интерфейсах сетевых устройств присутствуют адреса IPv6. Вне зависимости от того, маршрутизируются ли они за пределы локального сегмента, вам нужно ограничить доступ для обоих семейств адресов.

Результат запроса: устройства Cisco Nexus, на которых не указаны списки доступа для протокола IPv4 и (или) IPv6.

Поддерживаемые системы: Cisco NX-OS.

> **Примечание.** Для одного и того же устройства информация о линии vty и об интерфейсе mgmt0 выводится в разных строках таблицы. На Nexus 1000V списки управления доступом для IPv6 появились начиная с версии 5.2(1).

Управление с любых адресов для GAiA

Если у устройств Check Point GAiA в списке доверенных узлов присутствуют префиксы /0 (0.0.0.0/0 или ::/0), это означает, что управление устройством разрешено с любого адреса в соответствующем семействе адресов (IPv4 или IPv6). Вам нужно ограничить множество адресов, с которых разрешено управление устройством.

Результат запроса: устройства Check Point GAiA, на которых разрешено управление со всех узлов.

Поддерживаемые системы: Check Point GAiA.

> **Примечание.** Для устройств, попавших под условие фильтрации (наличие префиксов /0), выводится полный список доверенных узлов, упорядоченный по убыванию длины префикса.

5.3.3. Тайм-аут простоя

Эти параметры уменьшают риск того, что злоумышленник воспользуется оставленным надолго без присмотра компьютером с аутентифицированным сеансом управления устройством.

Тайм-аут простоя SSH не соответствует требованиям

Вам нужно установить тайм-аут простоя для SSH в соответствии с политикой безопасности вашей организации. В системном запросе используется пороговое значение в 600 секунд. Установленный тайм-аут не должен превышать это значение.

Результат запроса: устройства, на которых заданный тайм-аут простоя для протокола SSH превышает пороговое значение.

Поддерживаемые системы: Check Point GAiA, Check Point SecurePlatform, Cisco ASA.

> **Примечание.** Для всех перечисленных систем тайм-аут простоя для SSH не может быть отключен (нельзя установить значение 0). Для унификации между системами значение тайм-аута простоя приводится к секундам.

Тайм-аут простоя HTTPS не соответствует требованиям

Если вы используете веб-интерфейс управления, вам нужно установить тайм-аут простоя для HTTPS в соответствии с политикой безопасности вашей организации. В системном запросе используется пороговое значение в 600 секунд. Установленный тайм-аут не должен превышать это значение. Также тайм-аут не должен быть отключен (не должно быть установлено значение 0).

Результат запроса: устройства, на которых включена служба HTTPS и тайм-аут простоя не задан или превышает пороговое значение.

Поддерживаемые системы: Check Point GAiA, Cisco ASA, Juniper Junos OS.

> **Примечание.** Из всех перечисленных систем тайм-аут простоя для HTTPS может быть не задан только на Juniper Junos OS. Для унификации между системами значение тайм-аута простоя приводится к секундам.

Тайм-аут простоя на линиях не соответствует требованиям

Вам нужно установить тайм-аут простоя на линиях управления в соответствии с политикой безопасности вашей организации. В системном запросе используется пороговое значение в 10 минут. Установленный тайм-аут не должен превышать это значение. Также тайм-аут не должен быть отключен (не должно быть установлено значение 0).

Результат запроса: устройства, для которых тайм-аут простоя на линиях управления не задан или превышает пороговое значение.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Huawei VRP.

Тайм-аут простоя Telnet и SSH не соответствует требованиям (Cisco WLC)

Cisco WLC на базе AireOS использует единое значение тайм-аута простоя для сеансов Telnet и SSH. Вам нужно установить данный тайм-аут в соответствии с политикой безопасности вашей организации. В системном запросе используется пороговое значение в 10 минут. Установленный тайм-аут не должен превышать это значение. Также тайм-аут не должен быть отключен (не должно быть установлено значение 0).

Результат запроса: устройства Cisco WLC (AireOS), для которых тайм-аут простоя Telnet и SSH не указан или превышает пороговое значение.

Поддерживаемые системы: Cisco WLC (AireOS).

5.4. SNMP

Этот раздел содержит информацию о параметрах протокола SNMP.

Рекомендуется использовать протокол SNMPv3, поскольку он является более безопасным по сравнению с предыдущими версиями — SNMPv1 и SNMPv2c.

В этом разделе

Требования для SNMP версии 3 (см. раздел 5.4.1)

Требования для SNMP версий 1 и 2 (см. раздел 5.4.2)

5.4.1. Требования для SNMP версии 3

Устаревшие версии SNMP

Протоколы SNMPv1 и SNMPv2c передают данные в открытом виде. Вам нужно отключить устаревшие версии SNMP там, где это возможно.

Результат запроса: устройства, на которых активны протоколы SNMPv1 и SNMPv2c.

Поддерживаемые системы: Check Point GAiA, Cisco WLC (AireOS), Huawei VRP, Juniper Junos OS, Avaya (Nortel) NNOS.

> **Примечание.** Проверка осуществляется только для ОС, которые выводят список активных версий SNMP в явном виде, поэтому данная проверка не даст результатов для Cisco ASA, Cisco IOS, Cisco IOS XR и Cisco NX-OS.

Недостаточный уровень безопасности для групп

Более высокая безопасность SNMPv3 по сравнению с предыдущими версиями обеспечивается возможностями аутентификации и шифрования сообщений. Вам нужно для каждой группы SNMPv3 установить уровень безопасности AuthPriv.

Результат запроса: устройства, на которых при включенной службе SNMP отсутствуют группы SNMP или присутствуют группы SNMPv3 с моделью доступа, отличной от v3, и с уровнем безопасности, отличным от AuthPriv.

Поддерживаемые системы: Cisco ASA, Cisco IOS, Cisco IOS XE, Cisco IOS XR, Huawei VRP, Juniper Junos OS.

Протокол шифрования не соответствует требованиям

Более высокая безопасность SNMPv3 по сравнению с предыдущими версиями обеспечивается возможностями аутентификации и шифрования сообщений. Для каждого пользователя SNMPv3 вам нужно установить параметры приватности с использованием метода шифрования не хуже AES-128 или 3DES.

Результат запроса: пользователи SNMP, для которых задан протокол шифрования хуже AES-128 или 3DES или шифрование отсутствует.

Поддерживаемые системы: Alcatel AOS, Cisco ASA, Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Cisco WLC (AireOS), Huawei VRP, Juniper Junos OS, Avaya (Nortel) NNOS.

Не заданы списки доступа для пользователей (IPv4)

Применение списков доступа позволяет ограничить доступ по SNMP для избранной группы IP-адресов источника. Для каждого пользователя SNMPv3 вам нужно указать применяемый список доступа. Вы можете использовать этот запрос, если в сети отсутствует адресация IPv6 и достаточно ограничить доступ по IPv4.

Результат запроса: пользователи SNMP, для которых не задан список доступа по протоколу IPv4.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Huawei VRP.

> **Примечание.** Проверка для IOS XR аналогична другим системам и не учитывает настройки Management Plane Protection.

Не заданы списки доступа для пользователей (IPv4 и IPv6)

Применение списков доступа позволяет ограничить доступ по SNMP для избранной группы IP-адресов источника. Для каждого пользователя SNMPv3 вам нужно указать применяемый список доступа. Вы можете использовать этот запрос, если на интерфейсах сетевых устройств присутствуют адреса IPv6. Вне зависимости от того, маршрутизируются ли они за пределы локального сегмента, вам нужно ограничить доступ для обоих семейств адресов.

Результат запроса: пользователи SNMP, для которых не заданы списки доступа по протоколам IPv4 и IPv6.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Huawei VRP.

> **Примечание.** Проверка для IOS XR аналогична другим системам и не учитывает настройки Management Plane Protection.

Не заданы списки доступа для групп (IPv4)

Применение списков доступа позволяет ограничить доступ по SNMP для избранной группы IP-адресов источника. Для каждой группы SNMPv3 вам нужно указать применяемый список доступа. Вы можете использовать этот запрос, если в сети отсутствует адресация IPv6 и достаточно ограничить доступ по IPv4.

Результат запроса: группы SNMP, для которых не задан список доступа по протоколу IPv4; их модель и уровень безопасности.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Huawei VRP.

> **Примечание.** Проверка для IOS XR аналогична другим системам и не учитывает настройки Management Plane Protection.

Не заданы списки доступа для групп (IPv4 и IPv6)

Применение списков доступа позволяет ограничить доступ по SNMP для избранной группы IP-адресов источника. Для каждой группы SNMPv3 вам нужно указать применяемый список доступа. Вы можете использовать этот запрос, если на интерфейсах сетевых устройств присутствуют адреса IPv6. Вне зависимости от того, маршрутизируются ли они за пределы локального сегмента, вам нужно ограничить доступ для обоих семейств адресов.

Результат запроса: группы SNMP, для которых не заданы списки доступа по протоколам IPv4 и IPv6; их модель и уровень безопасности.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Huawei VRP.

> **Примечание.** Проверка для IOS XR аналогична другим системам и не учитывает настройки Management Plane Protection.

5.4.2. Требования для SNMP версий 1 и 2

Стандартные строки сообщества

Использование широко известных паролей, таких как private и public, в качестве строки сообщества SNMP позволяет злоумышленнику легко получить неавторизованный доступ к устройству. Вам нужно исключить использование таких паролей.

Результат запроса: устройства, на которых присутствуют стандартные строки сообщества SNMP, и уровень доступа для этих сообществ.

Поддерживаемые системы: Alcatel AOS, Check Point GAiA, Check Point SecurePlatform, Cisco ADE-OS, Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Cisco WLC (AireOS), Huawei VRP, Juniper Junos OS.

> **Примечание.** Некоторые ОС, такие как Cisco ASA и Avaya (Nortel) NNOS, не позволяют просматривать сконфигурированные строки сообщества SNMP. Для таких систем данная проверка не даст результатов.

Доступ на запись по SNMP

Доступ на чтение и на запись по SNMP позволяет удаленно управлять устройством. Для всех строк сообществ SNMP на устройстве вам нужно установить уровень доступа «Только чтение».

Результат запроса: сообщества SNMP с правами доступа на запись.

Поддерживаемые системы: Check Point GAiA, Check Point SecurePlatform, Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Cisco WLC (AireOS), Huawei VRP, Juniper Junos OS.

> **Примечание.** Некоторые ОС, такие как Cisco ASA и Avaya (Nortel) NNOS, не позволяют просматривать сконфигурированные строки сообщества SNMP. Для таких систем данная проверка не даст результатов.

Не заданы списки доступа для сообществ (IPv4)

Применение списков доступа позволяет ограничить доступ по SNMP для избранной группы IP-адресов источника. Для всех сообществ SNMP вам нужно указать применяемый список доступа. Вы можете использовать этот запрос, если в сети отсутствует адресация IPv6 и достаточно ограничения доступа по IPv4.

Результат запроса: сообщества SNMP, для которых не задан список доступа по протоколу IPv4, и уровень доступа для этих сообществ.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Huawei VRP.

> **Примечание.** Проверка для IOS XR аналогична другим системам и не учитывает настройки Management Plane Protection.

Не заданы списки доступа для сообществ (IPv4 и IPv6)

Применение списков доступа позволяет ограничить доступ по SNMP для избранной группы IP-адресов источника. Для всех сообществ SNMP вам нужно указать применяемый список доступа. Вы можете использовать этот запрос, если на интерфейсах сетевых устройств присутствуют адреса IPv6. Вне зависимости от того, маршрутизируются ли они за пределы локального сегмента, необходимо ограничить доступ для обоих семейств адресов.

Результат запроса: сообщества SNMP, для которых не заданы списки доступа по протоколам IPv4 и IPv6, и уровень доступа для этих сообществ.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Huawei VRP.

> **Примечание.** Проверка для IOS XR аналогична другим системам и не учитывает настройки Management Plane Protection.

5.5. Параметры журналирования

Служба журналирования отключена

Служба журналирования позволяет оперативно получать сообщения о событиях, связанных с безопасностью. Вам нужно включить службу журналирования на тех устройствах, где она отключена.

Результат запроса: устройства, на которых отключена служба журналирования.

Не задан сервер syslog (проверка по умолчанию)

Отправка сообщений syslog во внешнюю систему дает возможность долгосрочного хранения и анализа данных о событиях, связанных с безопасностью. Вам нужно настроить отправку сообщений на внешний сервер syslog.

Результат запроса: устройства, на которых не настроена отправка сообщений на внешний сервер syslog.

Поддерживаемые системы: Alcatel AOS, Cisco ADE-OS, Cisco ASA, Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Eltex ESR, Eltex MES (ROS), Fortinet FortiOS, HP Comware, Huawei VRP, Juniper Junos OS.

Уровень важности регистрируемых событий не соответствует требованиям (проверка по умолчанию)

Уровень важности регистрируемых событий должен быть установлен не ниже, чем informational (6).

Результат запроса: устройства, на которых заданный уровень важности регистрируемых событий не соответствует требованиям.

Поддерживаемые системы: Alcatel AOS, Cisco ADE-OS, Cisco ASA, Cisco IOS, Cisco IOS XE, Cisco IOS XR.

Уровень важности регистрируемых событий для сервера не соответствует требованиям

Для систем, в которых уровень важности регистрируемых событий настраивается для каждого сервера в отдельности, для каждого сервера syslog уровень важности регистрируемых событий должен быть установлен не ниже, чем informational (6).

Результат запроса: устройства и серверы syslog, для которых заданный уровень важности регистрируемых событий не соответствует требованиям.

Поддерживаемые системы: Cisco IOS XR, Cisco NX-OS, Eltex ESR, Fortinet FortiOS.

Примечание. Cisco IOS XR позволяет как задать общий уровень регистрируемых событий для направления «trap» (по умолчанию действует для всех серверов), так и указать значение для конкретного сервера. Таким образом, поскольку в конфигурации устройства присутствуют две точки контроля этого параметра, для IOS XR применимы обе проверки.

Уровень важности регистрируемых событий не соответствует требованиям (Junos)

Для каждого сервера syslog отдельно настраивается журналирование подсистем (facilities). Для каждой из них уровень важности регистрируемых событий должен быть установлен не ниже, чем informational (6).

Результат запроса: устройства Junos, а также серверы syslog и facilities, для которых указанный уровень важности регистрируемых событий не соответствует требованиям.

Поддерживаемые системы: Juniper Junos OS.

Уровень важности регистрируемых событий не соответствует требованиям (VRP)

Для каждого сервера syslog в качестве источника сообщений устанавливается канал инфоцентра, в рамках которого статус и уровень журналирования событий настраиваются для отдельных модулей (или для модуля по умолчанию, параметры которого распространяются на все подсистемы). Для всех каналов, связанных с серверами syslog, на всех указанных модулях журналирование событий должно быть включено и уровень важности регистрируемых событий должен быть установлен не ниже, чем informational (6).

Результат запроса: устройства Huawei VRP, а также серверы syslog и модули, для которых указанный уровень важности регистрируемых событий не соответствует требованиям.

Поддерживаемые системы: Huawei VRP.

Уровень важности регистрируемых событий не соответствует требованиям (Comware)

Для каждого сервера syslog в качестве источника сообщений устанавливается канал инфоцентра, в рамках которого статус и уровень журналирования событий настраиваются для отдельных модулей (или для модуля по умолчанию, параметры которого распространяются на все подсистемы). Для всех каналов, связанных с серверами syslog, на всех указанных модулях журналирование событий должно быть включено и уровень важности регистрируемых событий должен быть установлен не ниже, чем informational (6).

Результат запроса: устройства HP Comware, а также серверы syslog и модули, для которых заданный уровень регистрируемых событий не соответствует требованиям.

Поддерживаемые системы: HP Comware.

Параметры меток времени не соответствуют требованиям (проверка по умолчанию)

Метки времени в сообщениях позволяют коррелировать события и отслеживать сетевые атаки, затрагивающие более одного устройства. Для всех типов журналирования, поддерживаемых устройством, вам нужно настроить метки времени с абсолютным временем события, включая год.

Результат запроса: устройства и типы журналирования, для которых параметры меток времени не установлены или не соответствуют требованиям.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco WLC (AireOS), HP Comware, Huawei VRP.

> **Примечание.** В модели активов MaxPatrol VM параметры отметок времени приводятся к нормализованной форме. В этой форме тип временных меток, основанных на абсолютном времени, представлен значением datetime, а наличие года представлено как отдельная переменная, вне зависимости от актуального синтаксиса, используемого в конкретной ОС. В результатах запроса приводится как нормализованное, так и исходное представление значений, не соответствующих требованию (например, нормализованное «uptime», исходное «boot»).

Таблица 2. Поддерживаемые системы и синтаксис меток времени в соответствии с требованиями

Система	Синтаксис
Cisco IOS	**datetime** [msec] [localtime] [show-timezone] **year**
Cisco IOS XE	**datetime** [msec] [localtime] [show-timezone] **year**
Cisco IOS XR	**datetime** [msec] [localtime] [show-timezone] **year**
Cisco WLC (AireOS)	datetime
HP Comware	date | iso
Huawei VRP	date | format-date

Подробные указания по настройке источников событий для MaxPatrol VM содержатся в Руководстве по настройке источников.

Отключены метки времени (Cisco ASA)

Метки времени в сообщениях позволяют коррелировать события и отслеживать сетевые атаки, затрагивающие более одного устройства. Вам нужно включить метки времени в регистрируемых событиях.

Результат запроса: устройства Cisco ASA, на которых отключены метки времени в регистрируемых событиях.

Поддерживаемые системы: Cisco ASA.

5.6. Протоколы обнаружения соседей

Включен протокол CDP

Cisco Discovery Protocol — протокол, используемый устройствами Cisco для обнаружения соседей в сегменте локальной сети. Он полезен в случае отладочных работ, но представляет собой угрозу безопасности при штатном функционировании сети из-за количества раскрываемой информации и возможности DoS-атак. Вам нужно полностью отключить CDP на устройствах Cisco.

Результат запроса: устройства, на которых не отключен протокол CDP.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Cisco WLC (AireOS).

Включен протокол LLDP

Link Layer Discovery Protocol — протокол канального уровня, позволяющий сетевому оборудованию оповещать оборудование, работающее в локальной сети, о своем существовании и передавать ему свои характеристики, а также получать от него аналогичные сведения. Он полезен в случае отладочных работ, но представляет собой угрозу безопасности при штатном функционировании сети из-за количества раскрываемой информации и возможности DoS-атак. Вам нужно полностью отключить LLDP на устройствах.

Результат запроса: устройства, на которых не отключен протокол LLDP.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Eltex ESR, Eltex MES (ROS), HP Comware, Huawei VRP, Juniper Junos OS.

5.7. NTP

Задано менее двух серверов NTP

Для того чтобы время на устройстве соответствовало времени на всех остальных устройствах в сети, вам нужно настроить как минимум два NTP-сервера, внешних по отношению к устройству.

Результат запроса: устройства, на которых не запущена служба NTP или указано менее двух серверов NTP.

Поддерживаемые системы: Alcatel AOS, Check Point Gaia, Cisco ADE-OS, Cisco ASA, Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Eltex ESR, Eltex MES (ROS), HP Comware, Huawei VRP, Juniper Junos OS.

Аутентификация NTP не соответствует требованиям (проверка по умолчанию)

Важно, чтобы время на устройстве не могло стать объектом манипуляций злоумышленника, так как это открывает возможность для DoS-атак на службы, полагающиеся на точное время, атак повторного воспроизведения и другой злонамеренной деятельности. Аутентификация NTP позволяет удостовериться в аутентичности сервера и в том, что данные не были изменены в процессе передачи по сети. Вам нужно настроить аутентификацию NTP и ключи аутентификации.

Объем информации, выводимой запросом для каждого устройства, зависит от того, на каком этапе не выполняется данное составное требование:

1. Не включена аутентификация NTP — выводятся все серверы NTP, заданные на устройстве, независимо от их параметров, так как проблема не в параметрах серверов.
2. Отсутствуют заданные серверы NTP — поля, соответствующие серверу и ключам, не заполнены, устройство присутствует в списке.
3. Аутентификация NTP включена, но для части серверов не выполняются требования к ключам — выводятся только серверы, не отвечающие требованиям.

Если для сервера не задан номер ключа, в модели данных для него используется значение –1.

Результат запроса: устройства, для которых не включена аутентификация NTP или ключ аутентификации для серверов не указан, не определен или не входит в список доверенных.

Поддерживаемые системы: Cisco ADE-OS, Cisco ASA, Cisco IOS, Cisco IOS XE, Cisco IOS XR, Cisco NX-OS, Eltex MES (ROS), HP Comware, Huawei VRP, Juniper Junos OS.

> **Примечание.** В текущей реализации этой проверки существует ограничение. Синтаксис конфигурации большинства сетевых устройств позволяет задавать список доверенных ключей только в виде перечисления. Из поддерживаемых для данного требования систем исключение составляет только Cisco IOS, где список доверенных ключей также может содержать диапазоны номеров ключей (например, `ntp trusted key 4 - 7`). В текущем варианте реализации проверка вхождения номера ключа в список доверенных использует оператор сравнения. Такая проверка даст достоверный результат при сравнении с номерами доверенных ключей, перечисленными по одному (что является единственным вариантом задания доверенных ключей для всех поддерживаемых систем, кроме Cisco IOS); в случае же использования диапазонов сравнение будет производиться только с границами диапазона. Так, для приведенного выше примера ключи 4 и 7 будут считаться доверенными, а ключи 5 и 6 — нет, хотя в действительности они являются таковыми.

Аутентификация NTP не соответствует требованиям (AOS)

Важно, чтобы время на устройстве не могло стать объектом манипуляций злоумышленника, так как это открывает возможность для DoS-атак на службы, полагающиеся на точное время, атак повторного воспроизведения и другой злонамеренной деятельности. Аутентификация

NTP позволяет удостовериться в аутентичности сервера и в том, что данные не были изменены в процессе передачи по сети. Вам нужно настроить аутентификацию NTP и ключи аутентификации.

Результат запроса: устройства Alcatel AOS, для которых не включена аутентификация NTP или ключ аутентификации для серверов не указан или не входит в список доверенных.

Поддерживаемые системы: Alcatel AOS.

> **Примечание.** Alcatel AOS не позволяет просматривать определенные на устройстве ключи аутентификации NTP, поэтому из данного требования исключается проверка существования ключа. В остальном объем информации, выводимой запросом для каждого устройства, такой же, как и для требования по умолчанию.

5.8. Парольные политики

Не задан пароль для повышения привилегий

Привилегированный режим управления устройством должен быть защищен паролем. Вам нужно задать пароль для повышения привилегий пользователя.

Результат запроса: устройства, на которых не задан пароль для повышения привилегий.

Поддерживаемые системы: Cisco ASA, Cisco IOS, Cisco IOS XE, Huawei VRP.

> **Примечание.** Не все версии Huawei VRP поддерживают пароли для повышения привилегий. В список попадут все устройства Huawei VRP, на которых не задан пароль для повышения привилегий, вне зависимости от того, поддерживает ли устройство такую возможность. Также в список попадут все устройства, о которых известно, что их операционная система относится к списку поддерживаемых для данного запроса, и которые не были просканированы в режиме Audit, так как в этом случае список паролей на устройстве не будет заполнен.

Отключено шифрование паролей (Cisco IOS)

Шифрование паролей в конфигурационном файле предотвращает возможность получения паролей неавторизованными пользователями путем чтения конфигурации. Вам нужно включить службу шифрования паролей.

Результат запроса: устройства Cisco IOS, на которых не включена служба шифрования паролей.

Поддерживаемые системы: Cisco IOS, Cisco IOS XE.

Алгоритм шифрования паролей не соответствует требованиям (Junos OS)

Шифрование паролей в конфигурационном файле предотвращает возможность получения паролей неавторизованными пользователями путем чтения конфигурации. Вам нужно установить алгоритм шифрования паролей SHA-256 или более стойкий.

Результат запроса: устройства Junos OS, на которых установлен алгоритм шифрования паролей MD5 или SHA-1.

Поддерживаемые системы: Juniper Junos OS.

Минимальная длина пароля не соответствует требованиям

Отсутствие контроля за стойкостью паролей, которые назначают себе пользователи, может привести к успешной атаке перебора паролей. Вам нужно установить минимальную длину пароля в соответствии с политикой безопасности организации (рекомендуемое минимальное значение — 8 символов).

Результат запроса: устройства, на которых минимально допустимая длина пароля меньше порогового значения.

Поддерживаемые системы: Alcatel AOS, Check Point Gaia, Cisco ADE-OS, Cisco ASA, Cisco IOS, Cisco IOS XE, Cisco WLC (AireOS), Eltex ESR, Fortinet FortiOS, Juniper Junos OS.

> **Примечание.** На многих системах этот параметр имеет минимальный порог, ниже которого его значение нельзя установить. В частности, для Alcatel AOS, Eltex ESR и Fortinet FortiOS этот порог равен 8, что совпадает с пороговым значением в стандартном запросе, то есть требования стандартного запроса выполняются всегда. Отключенной проверке соответствует значение 0.

Минимальное количество символов для каждого символьного класса не соответствует требованиям

Отсутствие контроля за стойкостью паролей, которые назначают себе пользователи, может привести к успешной атаке методом перебора паролей. Набор возможных требований к стойкости паролей различается для различных систем. В частности, он включает в себя требование к минимальному количеству символов, присутствующих в пароле, для каждого из следующих символьных классов: заглавные буквы, строчные буквы, цифры, специальные (не алфавитно-цифровые) символы. Вам нужно установить минимально допустимое количество символов для каждого символьного класса в соответствии с политикой безопасности организации (рекомендуемое минимальное значение для каждого символьного класса — 1).

Результат запроса: устройства, на которых минимальное количество символов хотя бы для одного из символьных классов меньше порогового значения.

Поддерживаемые системы: Alcatel AOS, Cisco ADE-OS, Cisco ASA, Eltex ESR, Fortinet FortiOS, Juniper Junos OS.

Минимальное количество символьных классов не соответствует требованиям

Отсутствие контроля за стойкостью паролей, которые назначают себе пользователи, может привести к успешной атаке методом перебора паролей. Набор возможных требований к стойкости паролей различается для различных систем. В частности, он включает в себя требование к минимальному количеству символьных классов (заглавные буквы, строчные буквы, цифры, специальные (не алфавитно-цифровые) символы), которые должны присутствовать в пароле. Вам нужно установить минимальное требуемое количество символьных классов в соответствии с политикой безопасности организации (рекомендуемое минимальное значение — 3).

Результат запроса: устройства, на которых минимальное количество символьных классов, требуемых в пароле, меньше порогового значения.

Поддерживаемые системы: Check Point GAiA, Cisco WLC (AireOS), Eltex ESR, Juniper Junos OS.

Не запрещено использование имени пользователя в пароле

Отсутствие контроля за стойкостью паролей, которые назначают себе пользователи, может привести к успешной атаке методом перебора паролей. Набор возможных требований к стойкости паролей различается для различных систем. В частности, он включает в себя запрет на то, чтобы в пароле содержалось имя пользователя или его производные (например, буквы, составляющие имя пользователя, в обратном порядке или их произвольные анаграммы). Вам нужно включить данную проверку на тех устройствах, которые ее поддерживают.

Результат запроса: устройства, на которых не запрещено использование имени пользователя в пароле.

Поддерживаемые системы: Alcatel AOS, Cisco ADE-OS, Cisco WLC (AireOS).

Максимальное время действия пароля не соответствует требованиям (проверка по умолчанию)

Если не установить максимальное время действия пароля, у злоумышленника будет больше времени на то, чтобы подобрать пароль или воспользоваться ранее скомпрометированным паролем. Вам нужно установить максимальное время действия пароля в соответствии с политикой безопасности организации. Значение 0 означает отсутствие ограничения. Рекомендуемое максимальное значение — 90 дней.

Результат запроса: устройства, на которых максимальное время действия пароля не установлено или превышает пороговое значение.

Поддерживаемые системы: Alcatel AOS, Check Point GAiA, Cisco ADE-OS, Cisco ASA, Eltex ESR, Fortinet FortiOS, Juniper Junos OS.

Максимальное время действия пароля не соответствует требованиям (Cisco WLC)

Если не установить максимальное время действия пароля, у злоумышленника будет больше времени на то, чтобы подобрать пароль или воспользоваться ранее скомпрометированным паролем. Вам нужно установить максимальное время действия пароля в соответствии с политикой безопасности организации. Значение 0 означает отсутствие ограничения. Рекомендуемое максимальное значение — 90 дней.

Результат запроса: устройства Cisco WLC и классы пользователей, для которых максимальное время действия пароля не установлено или превышает пороговое значение.

Поддерживаемые системы: Cisco WLC (AireOS).

> **Примечание.** На устройствах Cisco WLC под управлением AireOS максимальное время действия пароля задается по отдельности для двух классов пользователей: «mgmt» (пользователи, управляющие устройством при помощи консольного или графического интерфейсов) и «snmpv3» (пользователи SNMPv3). В AireOS версии 7.4 и ниже классы пользователей отсутствуют, следовательно, максимальное время действия пароля пользователей не ограничено, поэтому такие устройства попадут в результаты запроса. Также в результаты запроса попадут устройства Cisco WLC, которые не были просканированы в режиме Audit из-за отсутствия данных о классах пользователей.

Максимальное время действия пароля не соответствует требованиям (Palo Alto)

Если не установить максимальное время действия пароля, у злоумышленника будет больше времени на то, чтобы подобрать пароль или воспользоваться ранее скомпрометированным паролем. Вам нужно установить максимальное время действия пароля в соответствии с политикой безопасности организации. Значение 0 означает отсутствие ограничения. Рекомендуемое максимальное значение — 90 дней.

Результат запроса: устройства Palo Alto и локальные пользователи, для которых максимальное время действия пароля не установлено или превышает пороговое значение.

Поддерживаемые системы: Palo Alto PAN-OS.

> **Примечание.** На устройствах Palo Alto максимальное время действия пароля задается как в глобальной парольной политике, так и в парольном профиле, который назначается пользователям. Значение, указанное в парольном профиле, имеет приоритет над глобальной парольной политикой. В модели активов MaxPatrol VM для устройств Palo Alto глобальная парольная политика не собирается, поэтому запросом вы можете проверить только парольные профили. Запрос выводит как тех пользователей, для которых в назначенном парольном профиле максимальное время действия пароля не установлено или превышает пороговое значение, так и тех, для которых не назначен парольный профиль.

Количество сохраняемых паролей не соответствует требованиям (проверка по умолчанию)

Если пользователь при очередной смене пароля укажет один из паролей, установленных ранее, злоумышленник сможет воспользоваться ранее скомпрометированным паролем. Вам нужно установить количество паролей, которые будут сохраняться в истории, в соответствии с политикой безопасности организации.

Значение 0 означает, что история паролей не сохраняется. Рекомендуемое минимальное значение — 4.

Результат запроса: устройства, на которых заданное количество сохраняемых паролей меньше порогового значения.

Поддерживаемые системы: Alcatel AOS, Check Point GAiA, Eltex ESR, Juniper JunOS.

Не запрещено повторное использование паролей (FortiGate)

Если пользователь при очередной смене пароля установит один из паролей, использованных ранее, злоумышленник сможет успешно воспользоваться ранее скомпрометированным паролем. Вам нужно запретить повторное использование паролей.

Результат запроса: устройства FortiGate, на которых разрешено повторное использование паролей.

Поддерживаемые системы: Fortinet FortiOS.

> **Примечание.** На устройствах FortiGate парольная политика может быть или включена, или отключена для всего устройства в целом (в последнем случае никакие параметры парольной политики не применяются). Использование парольной политики проверяется отдельным запросом.

Временная блокировка пользователей не соответствует требованиям (проверка по умолчанию)

Если адрес, по которому устройство принимает входящие управляющие подключения, доступен из внешней сети, злоумышленник может осуществить множество попыток подключения за короткий промежуток времени, чтобы вызвать отказ в обслуживании или получить доступ к устройству, подобрав имя пользователя и пароль. Вам нужно настроить параметры обнаружения повторных неудачных попыток входа в систему и временную блокировку пользователей в соответствии с политикой безопасности организации. Для количества повторных неудачных попыток входа значение 0 означает, что механизм обнаружения не активирован. Рекомендуемое максимальное значение — 3.

Результат запроса: устройства, на которых временная блокировка пользователей отключена или заданное количество повторных неудачных попыток превышает пороговое значение.

Поддерживаемые системы: Alcatel AOS, Check Point SecurePlatform, Cisco ADE-OS, Cisco IOS, Cisco IOS XE, Juniper Junos OS.

Примечание. Данный запрос проверяет сам факт включения механизма обнаружения повторных неудачных попыток входа в систему и временной блокировки пользователей и количество повторных неудачных попыток входа в течение интервала обнаружения. Значение интервала обнаружения (на тех системах, где этот параметр можно настроить) должно соответствовать установленному ограничению на количество повторных неудачных попыток входа, рекомендациям производителя и политике безопасности организации.

Временная блокировка пользователей не соответствует требованиям (Cisco WLC)

Если адрес, по которому устройство принимает входящие управляющие подключения, доступен из внешней сети, злоумышленник может осуществить множество попыток подключения за короткий промежуток времени, чтобы вызвать отказ в обслуживании или получить доступ к устройству, подобрав имя пользователя и пароль. Вам нужно настроить параметры обнаружения повторных неудачных попыток входа в систему и временную блокировку пользователей в соответствии с политикой безопасности организации. Для количества повторных неудачных попыток входа значение 0 означает, что механизм обнаружения не активирован. Рекомендуемое максимальное значение — 3.

Результат запроса: устройства Cisco WLC и классы пользователей, для которых временная блокировка отключена или заданное количество повторных неудачных попыток превышает пороговое значение.

Поддерживаемые системы: Cisco WLC (AireOS).

Примечание. На устройствах Cisco WLC под управлением AireOS параметры временной блокировки задаются по отдельности для двух классов пользователей: «mgmt» (пользователи, управляющие устройством при помощи консольного или графического интерфейсов) и «snmpv3» (пользователи SNMPv3). В AireOS версии 7.4 и ниже классы пользователей отсутствуют, следовательно, отсутствует временная блокировка пользователей, поэтому такие устройства попадут в результаты запроса. Также в результаты запроса попадут устройства Cisco WLC, которые не были просканированы в режиме белого ящика (модулем audit) из-за отсутствия данных о классах пользователей.

Временная блокировка пользователей не соответствует требованиям (Palo Alto)

Если адрес, по которому устройство принимает входящие управляющие подключения, доступен из внешней сети, злоумышленник может осуществить множество попыток подключения за короткий промежуток времени, чтобы вызвать отказ в обслуживании или получить доступ к устройству, подобрав имя пользователя и пароль. Вам нужно настроить параметры обнаружения повторных неудачных попыток входа в систему и временную блокировку пользователей в соответствии с политикой безопасности организации. Для количества повторных неудачных попыток входа значение 0 означает, что механизм обнаружения не активирован. Рекомендуемое максимальное значение — 3.

Результат запроса: устройства Palo Alto и локальные пользователи, для которых временная блокировка отключена или заданное количество повторных неудачных попыток превышает пороговое значение.

Поддерживаемые системы: Palo Alto PAN-OS.

> **Примечание.** На устройствах Palo Alto параметры временной блокировки задаются в профиле аутентификации, который назначается пользователям. Запрос выводит как тех пользователей, для которых в назначенном профиле аутентификации количество повторных неудачных попыток входа в систему не установлено или превышает пороговое значение, так и тех, для которых не назначен профиль аутентификации.

Парольная политика отключена (FortiGate)

На устройствах FortiGate парольная политика может быть или включена, или отключена для всего устройства в целом (в последнем случае никакие параметры парольной политики не применяются). Также отдельно задается применение парольной политики к администраторам устройства и к общим ключам IPSec. Вам нужно включить парольную политику на устройстве и применить ее к администраторам устройства.

Результат запроса: устройства FortiGate, на которых парольная политика отключена глобально или не применяется к администраторам устройств.

Поддерживаемые системы: Fortinet FortiOS.

6. Обращение в службу технической поддержки

Техническая поддержка продукта включает в себя следующие услуги:

- решение вопросов эксплуатации продукта, помощь в использовании его функциональных возможностей;
- диагностику сбоев продукта, включая поиск причины сбоя и информирование клиента о найденных проблемах;
- разрешение проблем с продуктом, предоставление решений или возможностей обойти проблему с сохранением всей необходимой производительности;
- устранение ошибок в продукте (в рамках выпуска обновлений к продукту).

Вы можете получать техническую поддержку на портале.

Этот раздел содержит информацию о способах и условиях получения технической поддержки.

В этом разделе

6.1. Техническая поддержка на портале

Портал предоставляет вам возможность создавать запросы на техническую поддержку.

Вы можете создать учетную запись на портале, используя адреса электронной почты, расположенные на официальном домене вашей организации. Вы также можете указывать другие адреса электронной почты для учетной записи в качестве дополнительных. Для оперативной связи укажите в профиле учетной записи название вашей организации и контактный телефон.

Портал содержит статьи базы знаний, новости обновлений продуктов Positive Technologies, ответы на часто задаваемые вопросы пользователей. Для доступа к базе знаний и всем новостям нужно создать на портале учетную запись.

Техническая поддержка на портале предоставляется на русском и английском языках.

6.2. Время работы службы технической поддержки

На портале технической поддержки вы можете круглосуточно создавать и обновлять запросы, читать новости продуктов и пользоваться базой знаний.

6.3. Как служба технической поддержки работает с запросами

При получении вашего запроса специалист службы технической поддержки классифицирует его (присваивает запросу тип и уровень значимости) и выполняет дальнейшие шаги по выполнению запроса.

В этом разделе

6.3.1. Предоставление информации для технической поддержки

При обращении за технической поддержкой по первому требованию специалиста Positive Technologies нужно предоставить:

— номер лицензии на использование продукта;

— файлы журналов и другие наборы диагностических данных, хранящихся в продукте;

— снимки экрана;

— результаты выполнения рекомендаций специалиста технической поддержки;

— каналы для удаленного доступа к продукту (по взаимному согласованию оптимального канала диагностики).

Positive Technologies не несет обязательств по оказанию технической поддержки в случае отказа предоставить указанную выше информацию.

Если информация по обращению не предоставлена в течение значительного времени (от двух недель с момента последней активности), специалист технической поддержки имеет право считать ваше обращение неактуальным и, уведомив вас, закрыть запрос.

6.3.2. Типы запросов

Специалист технической поддержки относит ваш запрос к одному из следующих типов.

Вопросы по установке, повторной установке и предстартовой настройке продукта

Подразумевается помощь в подготовке продукта к работе, ответы на вопросы на данном этапе эксплуатации продукта. Техническая поддержка по этим вопросам доступна в течение 30 дней с момента активации продукта.

Вопросы по администрированию и настройке продукта

Включают в себя вопросы, возникающие в процессе эксплуатации продукта, рекомендации по оптимизации и настройке параметров продукта.

Восстановление работоспособности продукта

В случае критического сбоя и потери доступа к основной функциональности продукта специалист Positive Technologies оказывает помощь в восстановлении работоспособности продукта. Восстановление заключается либо в помощи по установке продукта заново с потенциальной потерей накопленных до сбоя данных, либо в откате продукта на доступную резервную копию (резервное копирование должно быть настроено заблаговременно). Positive Technologies не несет ответственность за потерю данных в случае неверно настроенного резервного копирования.

Обновление продукта

Positive Technologies поставляет пакеты обновления в течение срока обновления, указанного в лицензии на продукт.

Positive Technologies не несет ответственности за проблемы, возникшие при нарушении регламентированного процесса обновления.

Устранение дефектов продукта

Если по результатам диагностики обнаружен дефект продукта, Positive Technologies обязуется предпринять разумные усилия по предоставлению обходного решения (если возможно), а также включить исправление дефекта в ближайшие возможные обновления продукта.

6.3.3. Время реакции и приоритизация запросов

Время реакции на запрос рассчитывается с момента получения запроса до первичного ответа специалиста технической поддержки с уведомлением о взятии запроса в работу.

Время обработки запроса рассчитывается с момента отправки уведомления о взятии вашего запроса в работу до предоставления описания дальнейших шагов по устранению проблемы либо классификации вопроса, указанного в запросе, как дефекта ПО и передачи запроса ответственным лицам для исправления дефекта.

Время реакции и время обработки зависят от указанного вами уровня значимости запроса (см. таблицу 3).

Специалист службы технической поддержки оставляет за собой право переопределять уровень значимости запроса по приведенным ниже критериям. Указанные сроки являются целевыми и подразумевают стремление и разумные усилия исполнителя для их соблюдения, но возможны отклонения от данных сроков по объективным причинам.

Таблица 3. Время реакции на запрос и время его обработки

Уровень значимости запроса	**Критерии значимости запроса**	**Время реакции на запрос**	**Время обработки запроса**
Критический	Аварийные сбои, полностью препятствующие штатной работе продукта (исключая первоначальную установку) либо оказывающие критическое влияние на бизнес	До 4 часов	Не ограничено
Высокий	Сбои, затрагивающие часть функциональности продукта и проявляющиеся в любых условиях эксплуатации либо оказывающие значительное влияние на бизнес	До 24 часов	Не ограничено
Обычный	Сбои, проявляющиеся в специфических условиях эксплуатации продукта либо не оказывающие значительного влияния на бизнес	До 24 часов	Не ограничено
Низкий	Вопросы информационного характера либо сбои, не влияющие на эксплуатацию продукта	До 24 часов	Не ограничено

Указанные часы относятся только к рабочему времени специалистов технической поддержки (времени обработки запроса).

6.3.4. Выполнение работ по запросу

По мере выполнения работ по вашему запросу специалист технической поддержки сообщает вам:

— о диагностике проблемы и ее результатах;

— о поиске решения или возможности обойти причины возникновения проблемы;

— о планировании и выпуске обновления продукта (если требуется для устранения проблемы).

Если по итогам обработки запроса необходимо внести изменения в продукт, Positive Technologies включает работы по исправлению в ближайшее возможное плановое обновление продукта (в зависимости от сложности изменений).

Работы по запросу считаются выполненными, если:

— предоставлено решение или возможность обойти проблему, не влияющая на производительность и критически важную функцию продукта;

— диагностирован дефект продукта, собрана техническая информация о дефекте и условиях его воспроизведения; исправление дефекта запланировано к выходу в рамках планового обновления продукта;

— проблема вызвана программными продуктами или оборудованием сторонних производителей, не подпадающих под гарантийные обязательства по продукту;

— проблема классифицирована как неподдерживаемая.

positive technologies

Positive Technologies — лидер рынка результативной кибербезопасности. Компания является ведущим разработчиком продуктов, решений и сервисов, позволяющих выявлять и предотвращать кибератаки до того, как они причинят неприемлемый ущерб бизнесу и целым отраслям экономики. Наши технологии используют более 3300 организаций по всему миру, в том числе 80% компаний из рейтинга «Эксперт-400». Positive Technologies — первая и единственная компания из сферы кибербезопасности на Московской бирже (MOEX: POSI), у нее более 170 тысяч акционеров.