MaxPatrol VM версия 2.5

Обзор новых возможностей

Дата редакции документа: 20.08.2024

Содержание

1. Главное в релизе

В этом разделе приведено краткое описание наиболее важных возможностей, появившихся в новой версии MaxPatrol VM.

1.1. Поиск веб-уязвимостей

Если в IT-инфраструктуре вашей организации используются веб-приложения, важно иметь возможность искать в них уязвимости.

Теперь вы можете это делать с помощью модуля WebEngine. Запуск задач на сбор данных с профилем WebEngine доступен только на коллекторах, установленных на Linux.

Подробности см. в разделах «Модуль WebEngine» документа Настройка источников и «Данные об уязвимостях» документа Синтаксис языка запросов PDQL.

1.2. Расчет уязвимостей в ПО внутри Docker-контейнеров

Если в вашей организации используется Docker, полезно учитывать уязвимости и в тех приложениях, которые запускаются из контейнеров.

Новая версия MaxPatrol VM может рассчитывать уязвимости в пакетах Ubuntu и Debian, содержащихся в образах контейнеров и контейнерах, которые запускаются на основе этих образов. С такими уязвимостями можно работать в штатном режиме, для этого реализован набор стандартных PDQL-запросов **Управление уязвимостями** → **Уязвимости контейнеров**.

1.3. Проверка подключения задачи аудита

Сбор данных с модулем Audit нагружает целевые активы и может замедлять их работу. Поэтому важно быть уверенным, что задача настроена правильно, еще до того, как она будет запущена.

В новой версии перед запуском задачи аудита вы можете проверить для нее подключение к целевым активам и транспортам. Проверка осуществляется для всех транспортов в профиле модуля, выбранного для задачи. Вы можете скачать результаты проверки подключения в CSV-файл.

Подробности см. в разделе «Запуск проверки подключения» Руководства оператора.

2. Новые возможности

В этом разделе перечислены новые возможности MaxPatrol VM и дано их краткое описание.

2.1. Запрещенное время сканирования

Сканирование может нагружать целевые активы, замедляя выполнение их основных задач. Теперь вы можете настроить запрещенное время для задач сканирования: как только оно начнется, сбор данных будет приостановлен, а когда закончится — возобновлен.

2.2. Отчет о результатах выполнения задачи

Чтобы понимать причины ошибок при выполнении задачи на сбор данных, важно иметь информацию о выполнении подзадач в составе этой задачи. Теперь вы можете скачать отчет о выполнении подзадач для отдельной задачи в формате XLSX.

2.3. Объединение задач в группы

Теперь вы можете объединять задачи по сбору данных в группы и выполнять действия со всеми задачами группы одновременно. Пользователи могут иметь доступ к группам задач в зависимости от назначенных привилегий.

2.4. Настройка количества выполняемых подзадач

В коллекторах существует ограничение на количество одновременно выполняемых подзадач для модулей. При достижении заданного максимального значения новые подзадачи ставятся в очередь на выполнение.

Теперь в интерфейсе MaxPatrol VM вы можете самостоятельно задать количество одновременно выполняемых подзадач для модулей.

2.5. Экспорт и импорт результатов сканирования

Теперь MaxPatrol VM поддерживает экспорт и импорт результатов сканирования, полученных по итогам запуска задач на сбор данных. Это делает возможным перенос результатов сканирования из территориально удаленных сетей и подразделений или физически изолированных сегментов сети в основной MaxPatrol VM.

2.6. Глобальный список исключений сетевых узлов

В IT-инфраструктуру организации могут входить сетевые узлы, которые запрещено сканировать или подключение к которым может вызывать отказ в обслуживании.

В таких случаях ранее в MaxPatrol VM необходимо было в каждой задаче на сбор данных указывать сетевые узлы, исключаемые из проверки.

Теперь MaxPatrol VM позволяет создавать списки исключений сетевых узлов, которые распространяются на все существующие и создаваемые задачи на сбор данных.

2.7. Доставка обновлений базы уязвимостей

Теперь MaxPatrol VM поддерживает обновление данных об уязвимостях, обнаруживаемых в режиме Pentest, с глобального сервера обновлений Positive Technologies.

2.8. Расширение возможностей расчета уязвимостей

Теперь MaxPatrol VM рассчитывает уязвимости в пакетах для операционных систем Ubuntu и Debian, обнаруженных в Docker-контейнерах.

2.9. Экспорт и импорт профилей, справочников и учетных записей

Для MaxPatrol VM разработана утилита на основе Ansible-скриптов для переноса профилей, справочников и учетных записей пользователей с одного MaxPatrol VM на другой.

Подробности см. в разделе «Экспорт и импорт пользовательских профилей» Руководства администратора.

2.10. Шаблоны для выгрузки данных об активах

В MaxPatrol VM реализована возможность выгружать данные об активах в файл формата XLSX с использованием стандартных и пользовательских шаблонов. Для этого в MaxPatrol VM добавлены новые стандартные PDQL-запросы и шаблоны.

2.11. Парольная политика и автоматическая блокировка пользователей

В PT MC реализована возможность настройки парольной политики и автоматической блокировки пользователей.

3. Технические особенности

Информация, представленная в этом разделе, поможет избежать возможных ошибок при обновлении и последующей работе с продуктом.

Существует ряд особенностей версии 2.5:

- Перед началом обновления до версии 2.5 необходимо обратиться в Positive Technologies и получить ключ инсталляции PT MC и файл лицензии MaxPatrol VM нового формата. Ключи и лицензии из комплекта поставки предыдущих версий продукта несовместимы с новым механизмом лицензирования.
- Версия 2.5 поддерживает обновление с версий 1.5, 2.0, 2.1.
- Версия 2.5 поддерживает интеграцию с PT NAD версий 10.1, 10.2, 10.3, 11.0, 11.1, 12.0.
- Версия 2.5 поддерживает установку на Astra Linux Special Edition 1.7.5 на базе ядра Linux версии 5.15 и Debian 10.3—10.13 на базе ядра Linux версии 5.10.
- Прежде чем приступать к обновлению MaxPatrol VM, рекомендуется остановить все задачи на сбор данных, а также убедиться, что на период обновления не запланирован запуск задач по расписанию. Это позволит избежать накопления очередей во время обновления, а также ошибок при выполнении задач после обновления.
- В параметрах подключения модуля NADSensor компонента MP NAD Sensor изменено значение порта по умолчанию. Теперь для подключения используется порт 5555.
- Увеличены установленные по умолчанию ограничения на количество одновременно выполняемых подзадач для модулей Audit и Pentest. Теперь одновременно могут выполняться 20 подзадач.
- Оптимизирована скорость загрузки виджетов. Теперь системные виджеты загружаются менее 5 секунд.

Особенности обновления с версии 2.1

При обновлении на версию 2.5 с версии 2.1 (версия системы ниже 26.2.11288) возможно изменение подсетей Docker-контейнеров, используемых ранее.

> **Примечание.** Определить подсети, используемые Docker-контейнерами MaxPatrol VM, вы можете с помощью команды `docker inspect $(docker network ls -q) -f '{{range.IPAM.Config}}{{.Subnet}}{{end}}'`.

Если для IT-инфраструктуры вашей организации важно сохранить используемую ранее подсеть, необходимо при обновлении роли Deployer указать в качестве значений параметров `CustomDockerAddressPool` и `CustomDockerNetworkSize` используемую ранее подсеть для Docker-контейнеров и ее размер соответственно. Инструкцию по изменению параметров роли вы можете найти в разделе «Изменение конфигурации роли» Руководства администратора.

4. Улучшения

В этом разделе описаны улучшения MaxPatrol VM новой версии.

Приоритет выполнения задач

Теперь задачи на сбор данных, запущенные вручную, имеют более высокий приоритет перед задачами на сбор данных, запущенными по расписанию: задачи по расписанию выполняются после завершения всех задач, запущенных вручную.

Новая страница «Топология»

Карта сети и расчет достижимости перенесены из карточки актива на новую страницу **Топология**.

Разметка пограничных сетей

Теперь вы можете отмечать сети, расположенные на границе IT-инфраструктуры организации, а также переименовывать сети на странице **Топология**.

Расширение возможностей расчета достижимости

Теперь при расчете достижимости учитываются правила проксирования в PT AF версии 3, а также правила проксирования в HAProxy.

Фильтрация в задаче на сбор данных с Active Directory

Появилась возможность задавать условия фильтрации объектов LDAP в задаче на сбор данных с профилем Microsoft Active Directory Audit. Для каждого типа собираемых данных реализовано отдельное поле для фильтра: фильтр для пользователей, фильтр для групп, фильтр для компьютеров.

Расширение аудита

Теперь вы можете расширить область сбора событий аудита. Для этого необходимо сформировать артефакт расширения аудита с дополнительными базовыми утилитами сбора в виде файла формата YAML и загрузить его в каталог коллектора.

Доработка роли Deployer

Теперь в состав роли Deployer входит утилита Get-RoleInstance, с помощью которой вы можете просматривать информацию об установленных экземплярах ролей. Зная идентификатор экземпляра роли, вы можете переконфигурировать этот экземпляр с помощью утилиты Start-Configuration, которая входит в состав роли Deployer.

Изменения параметров уведомлений

Теперь информация обо всех действиях с уведомлениями, которые пользователь выполняет на странице **Система** → **Уведомления**, отображается в PT MC в журнале действий пользователя.

Наименования столбцов в таблицах на виджетах

В таблицах на виджетах по активам теперь можно добавлять кириллические наименования столбцов.