GIS ГАЗИНФОРМ СЕРВИС

Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v. 3

Описание релиза v. 3.1.700

Санкт-Петербург, 2020

Описание релиза программного комплекса управления конфигурациями и анализа защищенности «Efros Config Inspector» v.3.1.700

Программный комплекс «Efros Config Inspector» релиз 3.1.700 (далее ПК «Efros Config Inspector» v.3).

О релизе:

Основными нововведениями релиза являются:

– поддержка сервером Efros CI работы на базе операционной системы Astra Linux Special Edition (Smolensk) v. 1.6, сертифицированной ФСБ, Минобороны и ФСТЭК России, позволяющей обрабатывать информацию ограниченного доступа;

– новый механизм управления лицензиями;

– оптимизация настройки пользовательских отчетов;

– расширенный список модулей устройств для которых обеспечивается предоставление актуальной информации об известных уязвимостях и угрозах;

– поддержка Cisco Firepower, с возможностями модуля анализа межсетевых экранов;

– доработанные модули поддержки сред виртуализации.

Также добавлен ряд функциональных улучшений, расширена поддержка устройств. Выполнены доработки для упрощения работы пользователей и оптимизации системы.

Новые возможности

1 Поддержка операционной системы Astra Linux Special Edition (Smolensk) v. 1.6

Реализована возможность работы серверной части ПК «Efros Config Inspector» v.3 на ОС Astra Linux Special Edition (Smolensk) v. 1.6.

2 Активация лицензий

Реализован переход на новую систему лицензирования. Сервер Efros CI использует механизм активации лицензий, выпущенных с помощью сервера лицензирования. Лицензии можно активировать как в online, так в offline режиме. Процесс активации интуитивно понятен и удобен.

Переход будет осуществляться поэтапно, с поддержкой старых ключей лицензий.

3 Оптимизация настройки пользовательских отчетов

Вкладка “Отчеты” в разделе “Настройки” была удалена. Возможность создавать пользовательские отчеты и назначать их применение на профилях и устройствах перенесены в раздел “Профили”. Управление профилями устройства прослеживаются на вкладке “Отчеты” выбранного устройства. Изменение работы от состояния наследования ведет к созданию профиля устройства и наоборот.

4 Обновление уязвимостей

Обновлены определения словарей проверки уязвимостей для устройств Cisco Ironport, Cisco UCM.

Добавлена возможность обновления проверок уязвимостей, из базы данных уязвимостей ООО «Газинформсервис», для модуля vCenter, устройств Cisco Firepower Management Center, Cisco NX-OS.

5 Виртуализация

Модуль vCenter:
Добавлена поддержка миграции ВМ.
Добавлена загрузка уязвимостей и состояния Lockdown mode при контроле целостности гипервизоров по протоколу HTTPS.

Модуль Hyper-V:
Добавлен отчет SCVMM 2008 Сетевая составляющая.

6 Поддержка устройств

Добавлена поддержка устройства Cisco Firepower Management Center.
Добавлена поддержка устройств Fortinet.
Добавлена поддержка устройства Check Point R80 Management Server.
Добавлена поддержка устройства Cisco NX-OS.

Обновлен отчет по политикам брандмауэра для модулей Cisco, Check Point, для устройства Dionis-NX версии 2.0.
В модуль Huawei добавлена поддержка модуля управления устройствами, проверки безопасности. Добавлен новый тип отчета по политикам брандмауэра.
Обновлено регулярное выражение для получения имени пользователя при изменении конфигураций Cisco ASA.

7 Общие доработки

Добавлен ряд улучшений интерфейса клиентской консоли:

– формы управления расписаниями раздела «Настройки»;
– интерфейса отображения и управления активными сессиями пользователей «Настройки» (вкладка Мониторинг сервера);
– окна восстановления и запуска операций;
– окна задания подсети при создании зоны в форме «Проверки межсетевых экранов» раздела «Настройки»;
– панели «Действия с устройствами» вкладки «Статус», раздела «Устройства»;
– вкладки «Конфигурации» формы настройки профилей;
– раздел «События»;
– вкладка «Проверки безопасности» раздела «Настройки»;
– вкладки активации и управления лицензией раздела «Настройки».

Исправленные ошибки:

– Ошибка удаления название фильтра в разделе «События» (Bug 28656);
– Ошибка при использовании выборки в архиве vCenter\ESXi (Bug 29903);
– Падение консоли после удаления расписания (Bug 27698);
– Модуль Hyper-V. Не загружается отчет "файлы виртуальной машины", если файлы ВМ расположены локально (Task 29954);
– Остановка сервера при включении политик МСЭ для Huawei (Bug 30052);
– Настройки. Отчеты. Неактивные кнопки дополнительных настроек (Bug 30075);
– Ошибка «Значение не может быть неопределенным. Имя параметра: source» при попытке сделать выборку из архива по отчетам о проверке (Bug 30078);
– Остановка сервера при обновлении модуля Cisco (Bug 30107);
– Ошибка при удалении требования политики МСЭ (Bug 30116);
– Ошибка при создании требования МСЭ, если выбран тип протокола "другой" (Bug 30119);
– Зависание обновления БДУ по расписанию (Bug 30120);
– Проверка политик безопасности для Huawei VRP: Не сохраняется измененное значение параметра 5.3.27 (Bug 30198);
– Остановка службы сервера после миграции БД (Bug 30356);
– Лицензии. Наличие лишней информации для восприятия результата ошибки (Bug 28116);
– Отсутствует ограничение номера порта в модулях Syslog и SNMP Trap серверов (Bug 28926);
– Standalone ESXi. Не работают кнопки в области "описание" (Bug 30108);
– Отсутствует описание версии для модуля Управление устройствами (Bug 30392);

– Наличие сообщения "Восстановление конфигурации" в режиме конфигурирования (Bug 30408);
– Мониторинг. Контроль изменений. Не происходит фильтрация для всех элементов, кроме статистики за месяц (Bug 29885);
– Ошибка удаления созданного с помощью фильтра отчета из профилей (Bug 28791);
– Ошибка при изменении настроек модуля Windows (Bug 30318);
– Не работает экспорт данных в отчете по зонному анализу МСЭ (Bug 30436);
– Ошибка редактирования расписания обновления БДУ, можно менять имя и описание, но изменения не применяются (Bug 30538);
– Статус модуля не передается на управляющий сервер при временной недоступности подчиненного (Bug 30626);
– Ошибка загрузки отчетов по расписанию при большом количестве устройств с проверками уязвимостей (Bug 30695);
– Ошибка использования общих словарей уязвимостей, при отключении одного из использующих его модулей (Bug 30707);
– Зонный анализ: Ошибка обрабатки правила после action return, goto (Bug 30852);
– Standalone ESXi. Ошибка загрузки отчета о проверке (Bug 30444);
– Модуль Windows v26. Отсутствует информация об изменениях в версии (Bug 30973);
– Cisco ASA. Ошибка при загрузке правил файрвола, содержащих hostname (Bug 30993);
– Ошибка отображения записей версий Cisco IOS-XE (Bug 30853);
– Ошибка загрузки отчета Linux (Bug 31499);
– Ошибка при тестировании нового пользовательского отчета (Bug 31592);
– Ошибка сервиса лицензирования. При нарушении условий онлайн лицензии ссылка в баннере ведет к старой форме лицензии (Bug 31745);
– Ошибка сервиса лицензирования. Баннер о нарушении условий лицензии не появляется и не исчезает без перезапуска сервера (Bug 31751);
– Ошибка сервиса лицензирования. Отсутствует подтверждение при удалении онлайн лицензии (Bug 31755);
– Ошибка сервиса лицензирования. Отсутствует английская локализация (Bug 31768);
– Ошибка сервиса лицензирования. После удаления лицензии старого типа кнопка добавления лицензии старого типа остается (Bug 31769);
– Ошибка сервиса лицензирования. После удаления лицензии период окончания демо лицензии сбрасывается до 0 дней (Bug 31770);
– Ошибка сервиса лицензирования. После добавления лицензии старого типа поля "О Лицензии" и кнопки Добавления\Удаления не появляются сразу (Bug 31771);
– Ошибка сервиса лицензирования. Лицензирование. Опечатка в окне подтверждения удаления лицензии старого типа (Bug 31776);
– Ошибка добавления нового доменного пользователя или группы (Bug 31832);
– Linux версия сервера. Модуль Azimut. Ошибка при выборке\экспорте отчета (Bug 31863);
– Linux версия сервера. Модуль Cisco. Ошибка при загрузке отчета "running-startup difference" и проверке соединения (Bug 31872);

– Linux версия сервера. Не работает экспорт отчетов в PDF, использующий Java (Bug 31883);
– Linux версия сервера. Остановка сервера при отключении модуля (Bug 31964).