

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

Описание релиза v. 3.1.800

# Описание релиза программного комплекса управления конфигурациями и анализа защищенности «Efros Config Inspector» v.3.1.800

Программный комплекс «Efros Config Inspector» релиз 3.1.800 (далее ПК «Efros Config Inspector» v.3).

## О релизе:

Основными нововведениями релиза являются:

- поддержка установки на операционную систему РЕД ОС (Муром) v. 7.2;
- поддержка 64 разрядных операционных систем;
- сервисный режим для контролируемых устройств;
- доработанный механизм управления доступом пользователей;
- доработанный модуль поддержки vCenter;
- поддержка KVM.

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

# НОВЫЕ ВОЗМОЖНОСТИ

## 1 Поддержка операционной системы РЕД ОС (Муром) v. 7.2

Реализована возможность установки и работы серверной части ПК «Efros Config Inspector» v.3 на ОС РЕД ОС (Муром) v. 7.2.

## 2 Поддержка 64 разрядных операционных систем

В состав дистрибутива ПК включен инсталлятор *Efros Config Inspector Console 3.1.800.x64.msi* для установки серверной части ПК «Efros Config Inspector» на 64 разрядные операционные системы.

## 3 Сервисный режим для контролируемых устройств

Реализована возможность перевода контролируемых устройств в сервисный режим, например, для их обслуживания и восстановления, без необходимости удаления учетной записи устройства с сервера. В сервисном режиме устройства не опрашиваются по расписанию.

## 4 Управление доступом

Добавлена возможность настройки ограничения на загрузку отчетов для пользователя с правами чтения.

Изменено описание и добавлена возможность назначать числовые параметры для настроек пользователя.

## 5 Поддержка KVM

Добавлена поддержка нового типа устройств виртуализации, гипервизор KVM. На Базе CentOS 6.5 и 6.10, RHEL 6.4 и 6.5, RHEL 7.3.

## 6 Доработка модуля vCenter

Добавлена опция выполнения команд VMWare VCSA через sudo, аналогично linux модулям.

Добавлены новые типы устройств для контроля файлов ESXi без использования API. Контроль целостности файлов только по SSH и только по HTTPS.

## 7 Поддержка устройств

Добавлена поддержка устройства Scada.

Добавлен отчет по уязвимостям для устройства Cisco Firepower Management Center.

Перенесены проверки Cisco ASA в новый, редактируемый формат.

Добавлены проверки безопасности Astra linux на основе Red-book.

Добавлены проверки безопасности Азимут Marlin по рекомендациям вендора.

Добавлена поддержка Азимут Marlin в модуль Управление устройствами.

## 8 Общие доработки

Добавлен ряд улучшений интерфейса клиентской консоли:

- формы «Профили» раздела «Настройки»;
- панели списка устройств раздела «Устройства»;
- формы «Настройки пользователей» раздела «Настройки», блок «Проверка сложности паролей»;
- вкладки «Отчеты» раздела «Устройства», форма настройки отчетов;
- формы «Обработчики событий» раздела «Настройки», окно «Использование»;
- формы «Расписания» раздела «Настройки», окно «Использование»;
- раздел «События», фильтрация по типу события;
- формы «Проверки безопасности» раздела «Настройки».

### Исправленные ошибки:

- Ошибка отображения выполнения последней операции с устройством в области «Описание» (Bug 30704);
- Отчет "Содержимое текстового файла" не доступен для создания нового требования проверки безопасности (Bug 31282);
- Ошибка сканирования сети в версия Linux сервера. (Bug 31880);
- Ошибка удаления большого количества устройств при использовании MS SQL (Task 32142);
- Ошибки обновления параметров лицензии на виртуальной машине (Bug 32012);
- Ошибка взаимодействия с СУБД MS SQL Server в Linux версии сервера (Bug 32097);
- Ошибка импорта требований проверок МСЭ (можно импортировать дублирующие требования) (Bug 32107);
- Ошибка при загрузке отчета по политикам МСЭ. Check Point R80 REST API. (Bug 32191);
- Ошибка применения фильтра при пустом типе события (Bug 31073);
- Ошибка при удалении расписания (отображается как событие удаления обработчика событий) (Bug 31552);
- Ошибка при создании отчета. Выбор/смена устройства. Кнопка "Сменить" скрыта за рамками окна (Bug 31573);
- Ошибка одновременной установки модулей Azimut и Linux (Bug 31939);
- Ошибка фильтрации событий по сообщению (Bug 31974);
- Ошибка отображения русского текста в отчетах, экспортированных в формат PDF. Linux версия сервера. (Bug 32002);
- Ошибка проверки уязвимостей сетевых устройств. Неточная проверка диапазонов (Bug 32067);
- Ошибка изменения настроек отчетов по проверкам (Bug 32086);
- Остановка сервера при одновременной установке модулей с одинаковым словарем уязвимостей, но разной ревизией (Bug 32127);
- Пустые значения в столбце Адрес в таблице устройств для выделенной группы (Bug 32166);
- Ошибка отображения в поле "Подробности" (под syslog сообщением не переведены названия строк) Вкладка "События" (Bug 32174);

- Ошибка отображения в поле "Подробности" (столбцы фиксированного размера). Вкладка "События". (Bug 32175);
- Ошибка отображения окна удаления окна обновить события. Вкладка "События". (Bug 32179);
- Ошибка загрузки отчета running-startup difference на устройстве Eltex MES. Linux версия сервера. Модуль Eltex. (Bug 32218);
- Ошибка при удалении стандарта МСЭ "Узел LinkedList не принадлежит текущему LinkedList" (Bug 30747);
- Ошибка записи версий Cisco IOS-XE (не нормализованы и не находятся в БДУ) (Bug 30853);
- Ошибка записи версий Cisco IOS-XE (не отображаются в property) (Bug 31567);
- Ошибка при обновлении модуля Linux (Bug 32011);
- Ошибка отображения syslog сообщений (объединение двух syslog сообщений в одно) (Bug 32172);
- Ошибка при загрузке отчета по политикам МСЭ. CheckPoint R80 REST API. (Bug 32191);
- Ошибка потребления памяти Efos Config Agent при проверках (Bug 32280);
- Ошибка функционирования сервера при парсинге Cisco ASA (Bug 32366);
- Ошибка отображения проверок политик CIS при сворачивании верхних вкладок (Bug 32541);
- Ошибка загрузки отчёта "Правила межсетевого экрана". Cisco FMC. (Bug 32596);
- Ошибка при задании некорректных имен пользователей (Bug 32620);
- Ошибка функционирования сервера при включении стандарта МСЭ для профиля Cisco ASA. Linux версия сервера. (Bug 32576);
- Ошибка при открытии экспортированного в PDF отчета (Bug 32159);
- Остановка сервера при загрузке отчетов Cisco IOS, подключенного как Cisco AsyncOS. Сервер. (Bug 32184);
- Ошибка консоли при импорте требований МСЭ (Bug 32269);
- Ошибка при проверке подключения. Модуль DATAPK v1.13 (Bug 32400);
- Пустой отчет "Потоки данных" для объектов защиты. Модуль DATAPK v1.13. (Bug 32416);
- Несоответствие типа ОС в feature файле для AIX и SunOS (Bug 32422);
- Неточная маска ввода (Bug 32453);
- Ошибка запуска в конфигурационный файл на Linux (Bug 32501);
- Ошибка загрузки отчета по уязвимостям для устройства EDS. Модуль Моха. (Bug 32521);
- Переполнение очереди syslog сообщений, часть сообщений пропущена (Bug 32525);
- Обозначение версии Cisco не обновлено с 79 на 80 (Bug 32539);
- Пропадание вкладки "Глоб. адр.-Внутр. адр." при сворачивании вкладки "Внутр. адр.-Глоб. адр.". (Bug 32574);
- Ошибка фильтрации событий при задании пустого условия для типа события (Bug 32575);
- Не работает онлайн и оффлайн активация. Linux версия сервера. (Bug 32577);
- Падение консоли при удалении всех правил (Bug 32578);
- Ошибка при конфигурировании устройств группы. При выборе другого типа устройств количество выбранных устройств не изменяется (Bug 32618);

- Ошибка проверки соединения с устройствами. Linux версия сервера. (Bug 32624);
- При удалении папки с устройствами в событиях отображается только удаление папки (Bug 32635);
- Дублирование событий запуска/остановки хоста при каждой 2й загрузке (Bug 32810);
- Ошибка при сворачивании вкладок большого отчета о проверке безопасности (пропадают некоторые вкладки) (Bug 31025);
- Ошибка функционирования сервера при парсинге acl Cisco ASA (Bug 32366);
- Ошибка отображения проверок политик CIS при сворачивании верхних вкладок (Bug 32541);
- Не отображается название редактируемого события (Bug 32646);
- Ошибка HTTP 401 в произвольные моменты времени. CiscoFMC (Bug 32832);
- Ошибка функционирования сервера при одновременной загрузке отчетов по расписанию и вызове "Отключить все" для модулей (Bug 32540);
- Опечатка в расписании обновления БДУ (Bug 30287);
- Ошибка при обновлении модуля Cisco (v79 - v81) (Bug 32642);
- Ошибка отображения баннера о работе устройства в сервисном режиме (корректно работает только на вкладке "Статус" устройства) (Bug 32644);
- Ошибка отображения табличных отчетов в выборке по отчетам в разделе "Устройства" (Bug 31540);
- Ошибка удаления профиля устройства в настройках при изменении всех настроек в соответствии с профилем по-умолчанию (Bug 32205);
- Поиск в профилях не работает для профилей верхнего уровня (Bug 32087);
- Ошибка при проверке соединения. Модули Cisco ACS, Avaya. Linux версия сервера (Bug 32850);
- Ошибка отображения заголовка уязвимости в отчете (выходит за границы окна) (Bug 29086);
- Лишние символы в пунктах контекстного меню в описании устройств (Bug 31128);
- Ошибка загрузки отчета backup конфигурации (Bug 32024);
- Ошибка при создании расписания (Bug 32188);
- Ошибка отображения в отчетах по проверкам политик безопасности количества пройденных проверок (Bug 32363);
- Расписание обновления базы уязвимостей не переводится при изменении языка консоли. Консоль (Bug 32426);
- Не выполняется отключение модуля "Управление устройствами" (Bug 32450);
- Ошибка отображения переключателей (по нижнему краю обрезаются переключатели в панели откл/вкл столбцов). Список устройств (Bug 32533);
- Пропадание вкладки "Глоб. адр.-Внутр. адр." при сворачивании вкладки "Внутр. адр.-Глоб. адр." (Bug 32574);
- Ошибка отображения при удалении папки с устройствами в событиях (отображается только удаление папки) (Bug 32635);
- Ошибка отображения русского текста в полученном файле при экспорте отчетов по уязвимости (русский текст отображается "#") (Bug 32670);
- Ошибка HTTP 429 при наличии множества объектов на устройстве CiscoFMC (Bug 32727);

- Некорректный тип отчетов в области подробности на вкладке события. Cisco FMC (Bug 32751);
- Некорректно отображается русский текст в отчете "Оптимизация правил" Cisco FMC (Bug 32753);
- Ошибка при разборе портов>, <. CheckPoint R80 (Bug 32868);
- Записи версий Cisco IOS-XE не отображаются в property (Bug 31567);
- Ошибка отображения вкладки «Profiles» (не переведены некоторые названия) (Bug 33011);
- Не работает восстановление конфигурации на устройствах (Bug 32813);
- Ошибка при анализе правил (ложное срабатывание при совместном нарушении правила) (Bug 33084);
- Некорректная обработка пересечений правил. Анализ МСЭ (Bug 33118);
- Неверное имя исполняемого файла. Linux версия сервера. Модуль 3Com (Bug 32847);
- Падение консоли при создании стандарта после поиска стандарта в МЭ (Bug 33060);
- Ошибка при обновлении модуля Cisco (v79 - v81) (Bug 32642);
- Ошибка экспорта отчетов и устройств в папку при использовании длинных имён устройств (Bug 33089);
- Ошибка при вызове "Подробнее" для уведомления (Bug 33052);
- Ошибка при загрузке модуля Cisco на сервер. Linux версия сервера (Bug 31970);
- Ошибка при переходе к сканированию (Bug 33057);
- Отсутствует проверка дубликатов имен для зон в проверках МСЭ (Bug 33122);
- При создании пользователя в поле e-mail отсутствует маска ввода (Bug 33151);
- Бесконечное появление ошибок при нажатии на "Настройки отчетов" в устройстве (Bug 33025);
- Ошибка экспорта отчетов при большом количестве устройств с одинаковым названием (Bug 33080);
- Неверное описание версий № 8, 13 на английском. ViPNet Coordinator (Bug 31299);
- Ошибка запуска консоли (Bug 32991);
- Ошибка при вызове описания модулей (Bug 32998);
- Не загружается отчет "Список виртуальных машин" на RELS 7.3. Модуль KVM. (Bug 33351);
- Ошибка включения модуля "Управление устройствами" при использовании онлайн лицензии (Bug 33702);
- Ошибка загрузки модулей не загружается на сервер Linux версия сервера. (Bug 33511);
- Ошибка при загрузке отчетов от имени пользователя с правами на чтение (Bug 33510);
- Ошибка отображения правила по умолчанию из "IPv4 Policy" Fortigate. Правила МЭ. (Bug 33373);
- Не учитывается таблица конфигурации CLI. Fortigate (Bug 33381);
- Ошибка при запуске консоли (Bug 33254);
- Некорректное сообщение об ошибке при неправильном вводе пароля (Bug 33255);
- Кнопка "Выполнить" неактивна при конфигурировании устройств (Bug 33707);

- Не работает добавление подчиненного сервера при использовании онлайн лицензии (Bug 33509);
- Падает сервер при загрузке отчета "настройки гипервизора" для вложенного устройства Host. vCenter (Bug 33515);
- Нет кнопки подключения к устройству по ssh и https. Fortinet. (Bug 33579);
- Невозможно активировать онлайн лицензию (Bug 33592);
- Перепутаны местами source port и destination port в service custom. Fortinet (Bug 33668);
- Ошибка при создании базы данных (Bug 33701).