ГАЗИНФОРМ СЕРВИС

Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v. 4

Описание релиза v. 4.5.100

Санкт-Петербург, 2021

Описание релиза программного комплекса управления конфигурациями и анализа защищенности «Efros Config Inspector» v.4.5.100

Программный комплекс «Efros Config Inspector» релиз 4.5.100 (далее – ПК «EfrosConfig Inspector» v.4).

О релизе:

Основные нововведения релиза:

- добавлена поддержка SCADA Zond2015, DeltaV, CENTUM VP и Tekon (SCADA АСУД-248);
- добавлены проверки безопасности для Juniper;
- добавлены проверки безопасности и уязвимости для модуля zVirt;
- добавлены проверки безопасности для виртуализации Брест;
- добавлены проверки безопасности для FortiOS;
- добавлена поддержка контроля FortiWLC и FortiSwitch в модуль Fortinet;
- добавлена возможность конфигурирования и восстановления конфигураций для Eltex ESR:
- поддержка контроля СУБД Oracle;
- добавлен контроль целостности компонентов ПК «EfrosConfig Inspector» v.4;
- доработан раздел **Отчеты**.

Также добавлен ряд функциональных улучшений. Выполнены доработки для упрощения работы пользователей и оптимизации системы.

Новые возможности

1 Поддержка SCADA Zond2015, DeltaV, CENTUM VP и Tekon (SCADA АСУД-248)

Добавлена поддержка при работе под ОС Windows следующих SCADA:

- Zond2015 (ООО «Газприборавтоматика»);
- DeltaV (Emerson);
- CENTUM VP (Yokogawa Electric Corporation);
- SCADA АСУД-248 (НПО «Текон-Автоматика»).

2 Проверки для Juniper, FortiOS, виртуализации Брест

Добавлены проверки безопасности в модули:

- Juniper (для JUNOS в новом редактируемом формате);
- Fortinet (для FortiOS);
- KVM (для виртуализации Брест).

3 Проверки и уязвимости для zVirt

Для устройств zVirt добавлены отчет по уязвимостям и проверки безопасности (для гипервизоров CentOS и Redhat).

4 Конфигурирование и восстановление Eltex ESR

Добавлена поддержка конфигурирования и восстановления конфигурации в модуль управления для устройств типа Eltex ESR.

5 Добавлен внешний модуль поддержки СУБД Oracle

Добавлен новый внешний модуль контроля СУБД Oracle версии 10g.

6 Поддержка устройств FortiWLC и FortiSwitch

В модуль Fortinet добавлена поддержка контроля новых типов устройств FortiWLC и FortiSwitch.

7 Периодический контроль целостности компонентов ПК «Efros Config Inspector» v.4

Добавлен периодический контроль целостности компонентов ПК «EfrosConfig Inspector» v.4: раз в 10 минут – Сервер, Windows Агент, Коллектор, раз в 5 минут – Клиентская консоль.

Возможные статусы проверки на целостность компонентов: целостность подтверждена, нарушена целостность. События нарушения целостности Сервера, Windows Агента и Коллектора фиксируются в журнале событий комплекса. При нарушении целостности в консоли отображаются уведомления с указанием компонента и вида нарушения: нарушена целостность файла <имя файла>, файл <имя файла> не найден, неизвестный файл <имя файла>. В тексте сообщения для Коллектора и Windows Агента содержится информация об адресе объекта, с которого пришло сообщение.

8 Новые типы отчетов раздела Отчеты

в разделе **Отчеты** добавлена возможность формирования шаблонов пользовательских отчетов типов:

– ***Проверки устройств*** – отчет содержит перечень проверок с результатами их выполнения для всех выбранных устройств, для каждой проверки приведено количество устройств, прошедших проверку успешно и не прошедших проверку, описание проверки и в блоке Устройства – список выбранных для отчета устройств с результатом выполнения проверки для каждого. При выборе имени устройства открывается карточка устройства;
– ***Уязвимости устройств*** – отчеты, содержащие перечень уязвимостей для устройств заданных типов. Отчет содержит перечень уязвимостей, выявленных хотя бы для одного из выбранных для отчета устройств. Для каждой уязвимости указано количество устройств, для которых она выявлена, описание уязвимости и в блоке Устройства – список этих устройств. При выборе имени устройства открывается карточка устройства;

9 Доработки интерфейса

Выполнены доработки интерфейса консоли для упрощения работы пользователей:

– в разделе **Отчеты** внесены изменения в правила формирования заголовка формы просмотра отчетов:
  а) при открытии отчета по шаблону (по двойному клику по имени шаблона) в заголовке формы просмотра отображается имя шаблона;
  б) при создании нового отчета или при открытии формы просмотра отчета через меню "Выполнить на основе", в заголовке формы просмотра отображается имя базового отчета, если базового отчета нет – тип отчета (например, "История изменений");
– добавлено графическое отображение состояния заблокированности для переключателя

;
– в разделе **Потоки** добавлены заглушки для списка триггеров и списка событий по триггеру на отсутствие в списке триггеров и событий по триггеру, а также на отсутствие подключения к серверу «Efros Security Center Flow Server»;
– добавлены заглушки для «пустого» поиска/фильтрации в деревьях объектов:
  а) **Устройства** - дерево устройств;

б) **Настройки** - Профили - дерево профилей;
в) **Настройки** - Проверки безопасности - дерево стандартов;
г) **Настройки** - Проверки межсетевых экранов - дерево стандартов.

– добавлены заглушки для «пустого» поиска/фильтрации в списках/таблицах объектов:

а) **Устройства** - вкладка ***Отчеты***;
б) **Устройства** - ***Отчеты*** - Отчет по проверкам безопасности;
в) **Устройства** - ***Отчеты*** - Отчет по уязвимостям;
г) **Устройства** - вкладка ***События***;
д) **Устройства** - вкладка ***Архив***;
е) **Отчеты** - Список отчетов;
ж) **События**;
з) **Настройки** - ***Обработчики событий***;
и) **Настройки** - ***Профили*** - список конфигураций;
к) **Настройки** - ***Профили*** - список проверок;
л) **Настройки** - ***Расписания***;
м) **Настройки** - ***Проверки безопасности*** - список требований внутри стандарта;
н) **Настройки** - ***Проверки безопасности*** - список требований в базе; требований
о) **Настройки** - ***Проверки межсетевых экранов*** - список требований внутри стандарта;
п) **Настройки** - ***Проверки межсетевых экранов*** - список зон;
р) **Настройки** - ***Модули***;
с) **Настройки** - ***Мониторинг задач*** (картинка меняется, а текст нет).

– в подразделе ***Коллекторы*** раздела **Настройки** для коллекторов с обнаруженным нарушением контроля целостности для статуса *Нет связи* добавлено отображение причины отсутствия связи: «*Нет связи (нарушена целостность)*»;

10 Общие доработки

Выполнены следующие доработки для оптимизации системы:

– в подразделе **Мониторинг задач** раздела **Настройки** добавлена возможность поиска и возможность фильтрации списка заданий/задач по состоянию и типу задач. В поиск включены все элементы заданий и задач раздела **Мониторинг задач**. В качестве результата выводятся все задачи и задания, соответствующие поисковому запросу;

– в подразделе **Мониторинг задач** раздела **Настройки** добавлено автоматическое обновление состояния загруженных на страницу заданий и задач, обновление выполняется по событиям изменения статусов на стороне сервера;

– в разделе **Отчеты** введено разделение шаблонов отчетов на

а) личные (шаблон доступен только создавшему его пользователю) – доступ к списку ***Личные*** раздела **Отчеты** имеют все пользователи, имеющие доступ к серверу ПК. Пользователи имеют возможность создания/редактирования/удаления личных шаблонов, формирования на их основе отчетов;

б) общие (шаблон доступен всем пользователям) – доступ к общим шаблонам зависит от прав доступа к настройкам контроля. Если назначены любые права из категории *Настройки контроля*, то пользователь может видеть общие шаблоны. Создавать и редактировать общие шаблоны пользователь может только при наличии прав *Управление*;

– в разделе **Отчеты** добавлена возможность внесения изменений в шаблон из окна просмотра отчета, сформированного по этому шаблону. Если у пользователя есть права на изменение шаблона, то в меню, открывающемся по кнопке ***Шаблон,*** ему доступен пункт *Сохранить*, если прав нет, то доступен только пункт *Сохранить как* и пользователь может создать только новый шаблон;

– для модуля Postgres(Jatoba) реализован механизм построения вложенных устройств. При опросе СУБД загружаются БД этой СУБД как вложенные устройства по аналогии с vCenter;

– доработан модуль по работе с zVirt:

а) добавлены типы в дерево (датацентр и кластер);

б) добавлено логирование в файл;

в) добавлен отчет со списком Vm;

г) добавлен отчет по уязвимостям;

д) добавлены проверки безопасности на основе набора для kvm (для гипервизоров CentOS и Redhat).

– доработан модуль AD в части контроля групп пользователей. В отчете «Группы безопасности» выполнены доработки:

а) названия приведены в соответствие с AD;

б) для групп сделана единственная вложенная таблица, куда включены вложенные пользователи и группы;

в) добавлено отображение вложенных групп;

г) использовано отображение значка пользователя и группы по аналогии с AD.

– в модуль управления Eltex для устройств Eltex ESR добавлена поддержка анализа правил, оптимизации:

а) добавлен отчет правил межсетевых экранов;

б) добавлена поддержка проверок межсетевых экранов;

в) добавлен отчет оптимизации.

Исправленные ошибки:

Идентификатор	Описание ошибки
Bug 50019	Модуль zVirt. Правки профилей и описания модуля.
Bug 50007	Linux. Модуль Oracle. Не загружаются отчёты
Bug 49968	Win-агент2000 не воспринимает переменные системы Windows в пути к файлу.
Bug 49747	Linux. Не работает модуль Check Point. Check Point R77.
Bug 49742	Linux. Не работает модуль zVirt.

Идентификатор	Описание ошибки
Bug 49726	Пропадают права на чтение настроек обработчика событий
Bug 49719	Linux. Модуль MS SQL. Ошибка загрузки отчёта "Аудит".
Bug 49677	Невозможно клонировать устройство.
Bug 49644	Linux. Невозможно добавить модуль Cisco ACS.
Bug 49453	Отсутствие записи в событиях о подключении к резервному серверу.
Bug 49452	Не блокируется кнопка импорта при отсутствии необходимых прав
Bug 49451	Падение службы WinAgent2000 при загрузке пользовательского отчета
Bug 49449	Не сохраняются значения выполнения правил в проверках для профилей устройств
Bug 49415	Неправильная заглушка при безрезультатном поиске уязвимостей на устройстве.
Bug 49394	Не запускается служба агента в Windows Server 2000 EN
Bug 49315	Ошибка одновременной работы модулей Cisco и модуля Huawei.
Bug 49295	Опечатка в compliance Cisco.
Bug 49200	Опечатка во всплывающей подсказке об ошибке в фильтре событий в разделе "События" и в разделе "Устройства" на вкладке "События"
Bug 49140	Linux. Отсутствует файл server_file_digests.xml
Bug 49058	Huawei. На карте сети отображаются не все настроенные интерфейсы
Bug 49036	Кнопка экспорта отображается как активная без соответствующих прав на использование
Bug 49034	Опечатка в разделе "Профили подключения".
Bug 49030	Linux. Запуск службы завершается падением в libsnmp++.so.33
Bug 48981	Раздел "Настройки". Отсутствует описание у раздела "Потоки".
Bug 48895	Пользовательские модули. Неполный текст в подсказке для поля "Privilege prompt"
Bug 48894	Пользовательский модуль. Опциональное поле "Новое приглашение" не может быть пустым
Bug 48893	Linux. Падение службы сервера из-за отсутствия ресурса snmp_routes
Bug 48891	Возможное закрытие сессии без подписки на событие при изменении статусов подчиненных серверов 2-ой вложенности (внуков)
Bug 48872	VipNet. В часть отчетов попадает команда для вывода информации
Bug 48870	В логах сервера неверно отображаются сообщения об ошибках
Bug 48862	При открытии раздела События выдается сообщение об ошибке
Bug 48858	Ошибка запуска сервера после подключения подчиненного сервера
Bug 48658	Не отображается изменение имени правила МСЭ.
Bug 48598	Ошибка при снятии выбора с сервера с уведомлениями

Идентификатор	Описание ошибки
Bug 48596	Зависание сервера промежуточного сервера при изменении действия в профиле нижнего серера
Bug 48593	Ошибка проверки соединения с подчинённым резервным сервером.
Bug 48584	Лицензирование. Непонятное описание ошибки активации лицензии.
Bug 48528	Непонятная ошибка при удалении профиля SNMP.
Bug 48521	DATAPK. Раздел "События". Тип событий. Русский текст в английской версии сервера и консоли.
Bug 48506	Vipnet. Ошибка парсинга Local Rules в firewall rules Objects.
Bug 48433	У недоступного подчинённого сервера и его устройств\групп не заблокированы кнопки действий.
Bug 48410	Проверки OVAL(vulnerability и compliance) получаемые от dpk 1.17 отсутствуют на ОЗ в ECI
Bug 48409	Не загружаются отчёты на ОЗ полученные от DATAPK 1.17
Bug 48405	Падение сервера при обновлении экрана коллекторов
Bug 48401	Скрытие недоступных типов устройств в поле выбора при добавлении нового устройства.
Bug 48392	Экспорт\импорт. В окне ввода пароля не разблокируется кнопка "применить".
Bug 48387	Нет проверки уникальности имени профиля аутентификации.
Bug 48246	Ошибка импорта профилей SNMP и аутентификации
Bug 48241	Мониторинг задач. Невозможно посмотреть лог операции "задача" с ошибкой загрузки.
Bug 48198	Alcatel. Уязвимости в БДУ без score и векторов.
Bug 48187	Eltex восстановление конфигурации. Пароль сервера SCP в логах операции отображается в открытом виде.
Bug 48184	Раздел отчёты. Не настроена правовая политика на просмотр общих отчётов.
Bug 48177	Мониторинг задач. Бесконечная загрузка в поле подробно у некоторых заданий.
Bug 48174	Поиск в сохранённых фильтрах отчётов не сохраняет поисковые запросы.
Bug 48159	Окно выбора устройств. При выборе всех найденных по поиску устройств в группе идёт проброс выбора на группу.
Bug 48154	Окно мультивыбора. Неправильное название кнопки.
Bug 48153	Раздел "Отчёты". Мультивыбор старого формата.
Bug 48132	Astra\Red OS. Ошибка загрузки отчётов с устройства ESXi OS ssh.
Bug 48086	После сохранении профиля аутентификации в разделе настройки устройств происходит ошибка аутентификации.

Идентификатор	Описание ошибки
Bug 48084	Русский текст в отчёте проверки подключения к устройству по SNMP
Bug 48060	Раздел "Отчёты". На подчинённом сервере невозможно сохранить отчёт "История изменений" и личный отчёт "Выборка".
Bug 48059	Раздел "Отчёты". Русский текст в английской версии консоли.
Bug 48057	Раздел "Отчёты". При переключении с подчинённого сервера на главный появляется ошибка
Bug 48043	В английской версии консоли название дополнительных действий во вкладке "Changelog" на русском языке.
Bug 48042	В английской версии консоли название окна "Подтверждение изменения отчёта" на русском языке.
Bug 48041	В английской версии консоли русские названия в поле "authentication type".
Bug 48039	Кнопка добавления профиля аутентификация находит на поле выбора профиля.
Bug 48031	При английской версии сервера русские названия в таблице изменений.
Bug 48014	В английской версии консоли подсказки проверок на русском языке
Bug 47995	Раздел "Отчёты". Отчёт "История изменений". Счётчик устройств в шапке привязан к переключателю "Устройства без изменений"
Bug 47993	Раздел "Отчёты". После удаления всех выбранных устройств из "Выборки" или "Истории изменений" отчёт открывается с ошибкой
Bug 47974	Vipnet. Падение сервера при изменениях в отчёте "Vipnet firewall rules and objects"
Bug 47949	Права пользователя на экспорт\импорт устройств.
Bug 47948	Мониторинг. При увеличении размера окна выбора устройств не изменяется окно контента в нём.
Bug 47938	Устройства. Опечатка и русский текст в английской версии консоли.
Bug 47931	Потоки. При нажатии на кнопку удаления триггера появляется ошибка.
Bug 47930	Потоки. Отсутствие заглушки во вкладке "Триггеры" и кнопки "Повторить"
Bug 47928	Мониторинг. В виджетах скрывающийся элемент имеет название соответствующее языковой версии консоли в которой он был заведён
Bug 47914	Отсутствует пробел в статусе выполнения задачи с ошибками
Bug 47911	Опечатка в тосте Selfcheck EfrosCI
Bug 47900	Возможность сохранения нового формата экспорта .eci с пустым паролем
Bug 47899	В окнах добавления фильтра отсутствуют отступы
Bug 47836	Модуль Linux. Отсутствует описание для версии 37
Bug 47824	Окно обновления консоли без названия в шапке. Опечатка в тексте.

Идентификатор	Описание ошибки
Bug 47794	Ошибка в названии действия обработчика "Создать Уведомление"
Bug 47713	Перестает отображаться текст плейсхолдера групп и устройств в настройках виджета
Bug 47700	Не работает кнопка Отмена при автоматическом обновлении консоли
Bug 47697	Ошибка доступа при входе в консоль под пользователем без прав на управление
Bug 47689	Мониторинг. Не отображается структура выбора устройств и групп для всех виджетов
Bug 47688	Опечатка в окне автоматического обновления консоли
Bug 47687	Происходит удаление пользовательских фильтров событий миграции БД
Bug 47680	Карта сети. Не отображаются имена, заданные для интерфейсов
Bug 47678	Карта сети. Не отображаются интерфейсы полученные через snmp
Bug 47677	Потоки. При открытии окна создания триггера ошибка
Bug 47670	Ошибка загрузки отчёта vCenter Настройки гипервизора
Bug 47585	Мониторинг. В консоли на английском языке виджет "Подчиненные сервера" имеет русские слова
Bug 47574	При подключении стандарта МЭ к профилю Vipnet xFirewall возникает ошибка
Bug 47526	Отсутствует подсказка в окне конфигурирования Eltex MES
Bug 47367	Профили. Не происходит обновление использования профилей устройства при изменении в профиле типа устройств
Bug 47220	Ошибка при вводе несуществующего значения в фильтра табличного XML-отчета
Bug 47108	Неинформативный текст ошибки при создании доменного пользователя.
Bug 47023	Фильтр по XML отчету. При фильтрации по булевому условию возникает ошибка.
Bug 46751	Ошибка при импорте устройств через файл с расширением .eci. Импортируются не все файлы
Bug 46750	Импортирование устройств файлом в формате .eci происходит с ошибками.
Bug 46694	Ошибка загрузки иконок устройств после обновления модуля
Bug 46231	Контроль прав доступа. Загрузка большого отчета завершается XML-ошибкой
Bug 45931	Vipnet. Отчёт "Firewall rules". Не показываются данные в некоторых столбцах.
Bug 45857	В английской версии консоли русское название ошибки доступа.
Bug 45653	Vipnet. Отчёт Справочники и ключи.

Идентификатор	Описание ошибки
Bug 45610	Ошибка при открытии отчёта "Vipnet firewall rules and objects"
Bug 45567	Пользователь с правами на чтение не получает ошибки "доступ запрещён" при сохранении изменений в окне "Настройка отчётов для устройств".
Bug 45471	Модуль VipNet не загружается отчет firewall rules show
Bug 45413	Сервер Эфроса рушится под Линуксом при попытке обновления модулей
Bug 45390	Правила МСЭ. При смене порядка правил, в отчете порядок правил не меняется.
Bug 45371	Ошибка доступа при открытии консоли под пользователем без прав на текущем сервере
Bug 44833	БДУ. Не отображаются цифровые значения для уязвимостей Alcatel
Bug 44644	Лагает индикатор загрузки модулей
Bug 43924	Ошибка "Последовательность не содержит элементов" при загрузке DPIDataFlows в модуле DATAPK
Bug 43718	Устройство AD domain. Описание ошибки непонятное.
Bug 41602	[Устройства] Опечатка в тексте отчета ус-ва
Bug 38016	Отсутствуют ограничения по диапазону числовых значений для настройки параметров учетной записи пользователей комплекса
Bug 29987	Некоторые отчеты vCenter в архиве отображаются только в виде дерева
Bug 17839	Пароль пользователя после операции изменения пароля пользователя отображается в открытом виде в логах VMwareESXiLoadCommand