ПРОТОКОЛ № 6264/2021

проведения совместных испытаний программного изделия «Программный комплекс «KOMRAD Enterprise SIEM» версии 4.1.33 и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6)

г. Москва 22 октября 2021 г.

1 Состав Рабочей группы

1.1 Рабочая группа в составе: Толстых С. А. - руководителя группы по тестированию на совместимость с ПО отдела по работе с технологическими партнерами департамента внедрения и сопровождения ООО «РусБИТех-Астра», Карпенко Д. И. - инженера отдела по работе с технологическими партнерами департамента внедрения и сопровождения ООО «РусБИТех-Астра».

2 Предмет испытаний

2.1 Рабочая группа составила Протокол о том, что в период с 20 по 22 октября 2021 года были проведены совместные испытания программного изделия «Программный комплекс «KOMRAD Enterprise SIEM» версии 4.1.33 (далее по тексту — ПИ «KOMRAD»), разработанного АО «НПО «Эшелон» и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6) (далее по тексту - Astra Linux 1.6.0), операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 20211008SE16 (далее по тексту - Astra Linux 1.6.9), разработанных ООО «РусБИТех-Астра».

3 Объект испытаний

3.1 На испытания был предоставлен архив «KOMRAD 4.1.33 (ФСТЭК).zip» с дистрибутивом ПИ «KOMRAD».

3.2 Для работы с веб-интерфейсом ПИ «KOMRAD» использовался веб-браузер «Mozilla FireFox» версии 90.0.2.

4 Ход испытаний

4.1 В ходе испытаний были проведены проверки Astra Linux 1.6.9, запущенной с ядрами:

«generic» версии 5.10.0-1045, версии 5.4.0-81 и 4.15.3-154;

«hardened» версии 5.10.0-1045, версии 5.4.0-81 и 4.15.3-154.

4.2 Процесс установки и удаления ПИ «KOMRAD» описан в Приложении № 1.

4.3 В Astra Linux 1.6.0 ПИ «KOMRAD» устанавливается с ошибками, вследствие чего не запускается и не функционирует.

4.4 ПИ «KOMRAD» не работает в режиме мандатного разграничения доступа.

4.5 В ходе совместных испытаний были проведены проверки функционирования ПИ «KOMRAD» Astra Linux 1.6.9 в объеме, указанном в Таблице 1.

Таблица 1 — Перечень проверок ОС

№ п/п	Наименование проверки	Результат испытания
	Обновление ОС	**Astra Linux 1.6.9**
1	Выполнение требований подразд. 17.2 документа «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1	Успешно
2	Установка ПИ «KOMRAD» в среду ОС, загруженную с ядром «generic», «hardened»	Успешно
3	Запуск, остановка выполнения ПИ «KOMRAD» в среде ОС, загруженной с ядром «generic», «hardened»	Успешно
4	Сбор событий Syslog в ПИ «KOMRAD»	Успешно
5	Соответствие предустановленной операционной системы дистрибутиву. Проверка выполнялась с использованием утилиты «fly-admin-int-check»	Успешно
6	Удаление ПИ «KOMRAD» из среды ОС запущенной с ядром «generic», «hardened»	Успешно
7	Выполнение требований п. 17.3.2 документа «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1	Успешно

5 Результаты испытаний

5.1 По результатам проведения совместных испытаний на совместимость установлено, что ПИ «KOMRAD» корректно функционирует в среде Astra Linux 1.6.9.

Вывод

Программное изделие «Программный комплекс «KOMRAD Enterprise SIEM» версии 4.1.33 совместимо с операционной системой специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 20211008SE16 с учетом пунктов 4.3, 4.4.

От ООО «РусБИТех-Астра»


Толстых С. А.


Карпенко Д. И.

Приложение № 1

к Протоколу № 6264/2021

Установка и удаление ПИ «KOMRAD»

1 Установка ПИ «KOMRAD»

1.1 Для установки ПИ «KOMRAD» воспользуйтесь инструкцией «НПЕШ.60010-03 99 Руководство администратора.pdf», инструкция доступна по ссылке: https://nas01.astralinux.ru/sharing/vu7iqjgfw

2 Удаление ПИ «KOMRAD»

2.1 Для удаления ПИ «KOMRAD» выполнить команды:

apt purge komrad-processor pauth-server komrad-server komrad-s3 incident-manager correlation-dispatcher komrad-bus komrad-scanner {file,snmp,xflow,syslog,sql}-collector

apt autoremove

rm -rf /etc/echelon /etc/sysstat /usr/share/doc/echelontls /usr/share/doc/komrad* /usr/share/doc/pauthctl /usr/share/doc/sqlx-collector /var/lib/echelon /usr/bin/komrad*

rm /etc/default/sysstat /etc/systemd/system/multi-user.target.wants/komrad-reactor.service /lib/systemd/system/komrad-reactor.service /lib/systemd/system/sqlx-collector.service /usr/bin/echelontls /usr/bin/pauthctl /usr/bin/sqlx-collector

2.2 Если необходимо удалить базу данных clickhouse, выполнить команды:

apt purge clickhouse-*

apt autoremove

rm -rf /etc/clickhouse-server /var/lib/clickhouse

rm /etc/security/limits.d/clickhouse.conf /etc/systemd/system/multi-user.target.wants/clickhouse-server.service /lib/systemd/system/sqlx-collector.service /usr/bin/clickhouse-git-import

2.3 Удалить дополнительно установленный пакет nmap:

apt purge nmap

2.4 Если необходимо удалить базу данных postgresql, выполнить команды:

apt purge postgresql*

apt autoremove

Приложение № 2

к Протоколу № 6264/2021

Перечень сокращений и определений

ПИ «KOMRAD» - программное изделие «Программный комплекс«KOMRAD Enterprise SIEM» версии 4.1.33

Astra Linux 1.6.0 - операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6)

Astra Linux 1.6.9 - операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.6) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 20211008SE16

ОС — операционная система

КСЗ — комплекс средств защиты

ПО - программное обеспечение

ПИ - программное изделие