ПРОТОКОЛ № 22673/2024

проведения совместных испытаний программного обеспечения «Security Capsule SIEM (Консоль)» версии 3.3 и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7)

г. Москва 28.04.2024

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 09.04.2024 по 28.04.2024 совместных испытаний программного обеспечения «Security Capsule SIEM (Консоль)» версии 3.3 (далее – ПО), разработанного ООО «ИТБ», и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) (далее – Astra Linux SE 1.7.0), включая Astra Linux SE 1.7.0 с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-1023SE17 (оперативное обновление 1.7.5) (далее – Astra Linux SE 1.7.5), разработанной ООО «РусБИТех-Астра».

2 Объект испытаний

2.1 Перечень компонентов, эксплуатировавшийся в ходе проведения данных испытаний, относящихся к ПО, представлен в Таблице 1.

Таблица 1 – Перечень компонентов, относящихся к ПО

Описание	Наименование	Версия	Контрольная сумма	Источник
Docker-образ с ПО	siemwebapplicationcert.tar	-	2120034c7c8d772c1b9184d023985eca71b84fc26ae1c56fcedb58c40fb3f9ba	Сторона разработчика ПО
Руководство оператора	SC_SIEM-PO_РукОператор_14_09_2023.docx	-	-	
Руководство администратора	SC_SIEM-PA_19_09_2023-сертифицированная.docx	-	-	

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности функционирования ПО в средах: Astra Linux SE 1.7.0, Astra Linux SE 1.7.5 в объеме, указанном в Приложении 1.

3.2 Перечень используемых репозиториев приведен в Приложении 2.

3.3 Неофициальные репозитории ПО для указанных сред не эксплуатировались.

3.4 С целью проведения проверок при включённом режиме ЗПС использовался файл открытого ключа разработчика ПО.

3.5 При функционировании ПО в среде Astra Linux SE 1.7.0 выявлены некритичные ошибки DIGSIG, не влияющие на работоспособность ПО.

3.6 Проверка корректности функционирования ПО в условиях ненулевого уровня конфиденциальности механизма мандатного разграничения доступа (далее – МРД) указанных сред не проводилась по причине отсутствия поддержки ПО соответствующей функциональности ОС. Информация об отсутствии упомянутой поддержки была заявлена стороной разработчика ПО.

3.7 Недопустимо использовать ПО в условиях мандатного разграничения доступа по причине несоответствия указаний п.17.2.4.4 «Руководство по КСЗ Ч. 1».

3.8 Проверка функционирования docker-контейнера с ПО в непривилегированном режиме (rootless) в средах Astra Linux SE 1.7.0, Astra Linux SE 1.7.5 не проводилась.

3.9 Проверка на наличие уязвимости docker-образа и контейнера ПО в среде Astra Linux SE 1.7.0 не проводилась.

3.10 Проверка функционирования ПО при включенном механизме МКЦ в средах Astra Linux SE 1.7.0, Astra Linux SE 1.7.5 не проводилась.

3.11 Проверка функционирования контейнера на пониженном уровне МКЦ (виртуализация) в средах Astra Linux SE 1.7.0, Astra Linux SE 1.7.5 не проводилась.

3.12 ПО затрагивает требования по условиям функционирования п.17.3.2.1 «Руководство по КСЗ Ч. 1». Данные требования соблюдаются.

4 Результаты испытаний

4.1 ПО корректно функционирует в средах: Astra Linux SE 1.7.0, Astra Linux SE 1.7.5.

5 Вывод

5.1 ПО и операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) совместимы, принимая во внимание информацию, содержащуюся в разделах 3, 4 и Приложении 2.

6 Состав рабочей группы и подписи сторон

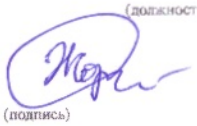
6.1 Данный протокол составлен участниками рабочей группы:

Жорин А. А. – главный специалист по внедрению ООО «ИТБ».

ООО «ИТБ»

главный специалист по внедрению

(должность)



(подпись)

Жорин А. А.

(фамилия, инициалы)

Приложение 1 к Протоколу № 22673/2024

Перечень проверок совместимости ПО и Astra Linux SE 1.7.0, Astra Linux SE 1.7.5

№ п/п	Наименование проверки	Результат проверки ПО и Astra Linux SE					
		1.7.0 с ядром ОС	1.7.5 с ядром ОС				
		5.4.0-54-generic	5.4.0-162-generic	5.10.190-1-generic	5.15.0-83-generic	5.15.0-83-lowlatency	6.1.50-1-generic
1.	Установка ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
2.	Запуск, остановка выполнения ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
3.	Функционирование ПО в среде ОС в рамках сценария проверки минимальной базовой функциональности	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
4.	Функционирование ПО при включенном механизме МКЦ в рамках сценария проверки минимальной базовой функциональности	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась
5.	Проверка функционирования контейнера на пониженном уровне МКЦ (виртуализация)	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась
6.	Функционирование ПО в рамках сценария эксплуатации в условиях ненулевого уровня конфиденциальности механизма МРД	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась
7.	Проверка функционирования docker-контейнера с ПО в непривилегированном режиме (rootless)	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась	Не проводилась
8.	Проверка на наличие уязвимости docker-образа и контейнера ПО	Не проводилась	Успешно	Успешно	Успешно	Успешно	Успешно
9.	Отсутствие ошибок в файл журнале docker	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
10.	Отсутствие нарушений требований подраздела 17.3 «Руководство по КСЗ Ч. 1»	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
11.	Соответствие объектов ФС ОС дистрибутиву ОС при эксплуатации ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
12.	Удаление ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
13.	Функционирование ПО в условиях включённого механизма ЗПС в рамках сценария проверки минимальной базовой функциональности	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
14.	Отсутствие нарушений требований подраздела 17.2 «Руководство по КСЗ Ч. 1»	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно

Приложение 2 к Протоколу № 22673/2024

Инструкция по установке и удалению ПО в средах: Astra Linux SE 1.7.0, Astra Linux SE 1.7.5

1 Используемые репозитории:

в Astra Linux SE 1.7.0:

- deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.0/repository-base/ 1.7_x86-64 main contrib non-free

в Astra Linux SE 1.7.5:

- deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-base/ 1.7_x86-64 main contrib non-free

2 Установка ПО:

2.1 выполнить системные команды, действия:

Выполнить действия по установке ПО «Security Capsule SIEM (Коррелятор и Сборщик)».

В конфигурационном файле postgresql.conf задать значения параметров ac_ignore_socket_maclabel = false, enable_bitmapscan = off.

Выполнить перезапуск сервиса и задать пароль vfr$%tgb12 пользователю postgres.

Распаковать архив с образом docker и перейти в каталог siemwebapplicationcert:

```
tar xf siemwebapplicationcert.tar.gz
cd siemwebapplicationcert/
```

Выполнить загрузку образа:

```
sudo docker load -i siemwebapplicationcert.tar
```

Создать сеть для контейнера:

```
sudo docker network create --opt com.docker.network.bridge.name=br000 --driver bridge --subnet 172.16.211.0/26 siem_net
```

Подключить токен guardant и определить адрес устройства:

```
lsusb
```

Внести изменения в файл siem/appsettings.json в параметры «Host=IP-address-psql» и «Password=password-user-psql».

Выполнить запуск контейнера:

```
sudo docker run -itd --name siemwebappcert-srv --network siem_net --device=/dev/bus/usb/001/002 -p 0.0.0.0:8000:80 -v /home/u/siem/siemwebapplicationcert/siem/appsettings.json:/app/appsettings.json -v
```

/home/u/siem/siemwebapplicationcert/siem/appsettings.enc:/app/appsettings.enc -v /home/u/siem/siemwebapplicationcert/siem/logs:/app/logs siemwebapplicationcert:latest

3 Удаление ПО:

3.1 выполнить системные команды, действия:

sudo docker stop <id-контейнера>

sudo docker rm <id-контейнера>

sudo docker rmi <id-образа>

sudo apt purge -y postgresql

Приложение 3 к Протоколу № 22673/2024

Перечень используемых сокращений и определений

«Руководство по КСЗ Ч. 1» – документ «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 1» РУСБ.10015-01 97 01-1;

Astra Linux SE 1.7.0 – операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7);

Astra Linux SE 1.7.5 – операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности БЮЛЛЕТЕНЬ № 2023-1023SE17 (оперативное обновление 1.7.5);

ЗПС – замкнутая программная среда ОС;

КСЗ – комплекс средств защиты;

МКЦ – мандатный контроль целостности ОС;

МРД – мандатное управление доступом ОС;

ОС – операционная система;

ПО – программное обеспечение «Security Capsule SIEM (Консоль)» версии 3.3;

Docker - программное обеспечение для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации;

Docker-образ – неизменяемый образ по шаблону которого создается docker-контейнер;

Docker-контейнер – контейнер, созданный на основе docker-образа;

Контейнер – изолирования среда с упакованным кодом и зависимостями.