ПРОТОКОЛ № 24630/2024

проведения совместных испытаний программного обеспечения «RT Protect EDR» версия агента 1.5, версия сервера 1.20 и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7)

г. Москва 10.09.2024

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 08.08.2024 по 10.09.2024 совместных испытаний программного обеспечения «RT Protect EDR» версия агента 1.5, версия сервера 1.20 (далее – ПО), разработанного АО «РТ-Информационная безопасность», и операционной системы 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) (далее – Astra Linux SE 1.7.5), разработанной ООО «РусБИТех-Астра».

2 Объект испытаний

2.1 Перечень компонентов, эксплуатировавшихся 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	docker.rt-protect.ru:5000/edr-backend/djangoapp	1.20.1	afaeb45755f6e4c556b195a6f2465883ae9e9831e56a13f12416442cf04d73ed	docker.rt-protect.ru
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/ioa-webapi	1.2.5	ba5943e6a70e49504679725759c1fddb91d75cef2271169fa0b3d9da629faa90	docker.rt-protect.ru
Docker-образ с ПО	docker.rt-protect.ru:5000/main/eas-front	2.38.22	ae2770e36bc659f2e623036f42dbd9160c3c82e100567e498618f8aee9f6d414	docker.rt-protect.ru
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/worker	1.20.0	847c6232bb10d6031b3f7950229709aea66cce33b4611c182019e719603445c9	docker.rt-protect.ru
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-	1.1.1	457fe5ffa4a24774546d439dd7493de18798eb72be927d6abf8	docker.rt-protect.ru

	backend/webserver		7bf09ac6bd978	
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/loadbalancer	1.1.0	9c72a1a27d12a53cbfd201dcbe17aeed7c0deaf7426cfaea8cc5ae4f9de131e2	docker.rt-protect.ru
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/loadbalancer	2.0.0	7d0c3a0582053636ae910f93f27161aa0e8754567cbef7cc5c9523f0b0e80f93	docker.rt-protect.ru
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/eventq	1.0.2	99ac9dd658d1fdb7b42b70cf7ce98e12a53d509c082fb1416078aba67c6cb0f1	docker.rt-protect.ru
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/rating-dbmigrator	1.7.1	f3160bc9329bd08070cb3cedf0e64df1a81459ae7340a3e5aa97ef019bd9b0b4	docker.rt-protect.ru
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/rating-webapi	1.7.1	7640505ac943589f0e82167c13c4544fe047d33545d35ecaf878199297bfeb2e	docker.rt-protect.ru
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/rating-worker	1.7.1	8dead3d74baceab6491a0d2ac51daf8452c9dc160433dee5ddde858c6c9a7ee4	docker.rt-protect.ru
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/elasticsearch	1.1.1	4a74d9a0892d8323e6f8229755f40fcb3cd68e4e108ddefec3e4406a787cf7c7	docker.rt-protect.ru
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/minio	1.0.1	80ca4834355ebc795d4b56fbca19e6d30eb79433cbe5facd8e7565dd8a5e8019	docker.rt-protect.ru
Docker-образ с ПО	docker.rt-protect.ru:5000/edr-backend/cache	1.0.1	40f8931b3e00fcffd83a3c23198b261ad3188abac89faad1c03591c47a126baa	docker.rt-protect.ru
Официальное руководство по эксплуатации ПО	Руководство администратора	1.0.19	-	https://cloud.rt-ib.ru/index.php/s/NSAPRqg8NYXF9r8

3 Ход испытаний

3.1 В ходе проведения настоящих испытаний были выполнены проверки корректности функционирования ПО в среде Astra Linux SE 1.7 в объеме, указанном в Приложении 1.

3.2 Перечень используемых репозиториев приведен в Приложении 2.

3.3 ПО не содержит исполняемых ELF/PE32-файлов. Внедрение ЭЦП для проверки работы с активным механизмом ЗПС не требуется.

3.4 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.

4 Результаты испытаний

4.1 ПО корректно функционирует в среде Astra Linux SE .

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:

Жуков А. К. – Руководитель Департамента сервисов и продуктов АО "РТ-Информационная безопасность";

Сафонов К.А. – Инженер Центра мониторинга и реагирования на компьютерные инциденты АО "РТ-Информационная безопасность";

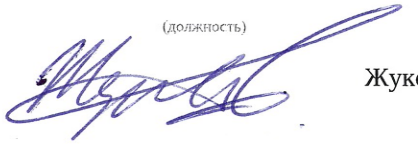
Валеева З.У. – Ведущий специалист Центра мониторинга и реагирования на компьютерные инциденты АО "РТ-Информационная безопасность";

Качаев З.К. – Аналитик Центра мониторинга и реагирования на компьютерные инциденты АО "РТ-Информационная безопасность".

АО "РТ-Информационная безопасность"

Руководитель Департамента сервисов и продуктов

(должность)



Жуков А.К.

Приложение 1 к Протоколу № 24630/2024

Перечень проверок совместимости ПО и Astra Linux SE 1.7

№ п/п	Наименование проверки	Результат проверки ПО и Astra Linux SE 1.7 с ядром ОС				
		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
2.	Эксплуатация ПО	Успешно	Успешно	Успешно	Успешно	Успешно
3.	Удаление ПО	Успешно	Успешно	Успешно	Успешно	Успешно
4.	Требования безопасности ALSE	Успешно	Успешно	Успешно	Успешно	Успешно
5.	Механизм безопасности ЗПС	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно
6.	Механизм безопасности МКЦ	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно
7.	Механизм безопасности МРД	Не проводилось	Не проводилось	Не проводилось	Не проводилось	Не проводилось
8.	Механизм безопасности rootless	Успешно	Успешно	Успешно	Успешно	Успешно

Приложение 2 к Протоколу № 24630/2024

Инструкция по установке и удалению ПО в среде Astra Linux SE 1.7

1 Используемые репозитории:

в Astra Linux SE :

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

2 Установка ПО:

2.1 выполнить системные команды, действия:

sudo apt update

sudo apt update

sudo apt install ansible sshpass openssh-server

ssh-keygen -t rsa -b 4096

ssh-copy-id user@ip

ansible-playbook edr-install --extra-vars "@config/default/config.yml" -i ip, -u username --ask-become-pass

3 Удаление ПО:

3.1 выполнить системные команды, действия:

docker container stop $(docker ps -a -q)

docker container prune

Приложение 3 к Протоколу № 24630/2024

Перечень используемых сокращений

Astra Linux SE – операционная система специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7) с установленным оперативным обновлением безопасности ;

ЗПС – замкнутая программная среда;

МКЦ – мандатный контроль целостности;

МРД – мандатное управление доступом;

ОС – операционная система;

ПО – программное обеспечение «RT Protect EDR» версия агента 1.5, версия сервера1.20.