ПРОТОКОЛ № 22246/2024
проведения совместных испытаний программного обеспечения «BI.ZONE EDR Server» версии 1.32.0 и операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01 (очередное обновление 1.7)

г. Москва 04.04.2024

1 Предмет испытаний

1.1 В настоящем протоколе зафиксирован факт проведения в период с 15.02.2024 по 04.04.2024 совместных испытаний программного обеспечения «BI.ZONE EDR Server» версии 1.32.0 (далее – ПО), разработанного ООО «БИЗон», 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, эксплуатировавшихся в ходе проведения данных испытаний, относящихся к ПО, представлен в Таблице 1.

Таблица 1 – Перечень компонентов, относящихся к ПО

Описание	Наименование	MD5	Источник
Файл программного пакета дистрибутива ПО	edr-distribs.tar.gz	2f0dad750352b26c773cd4e3c75a0ac9	Сторона разработчика ПО
Файл архива, содержащий файлы дистрибутивов дополнительных модулей ПО	edr-modules.tar.gz	0127fe03c5ed77c85a5607b25c761ff1	Сторона разработчика ПО
Официальное руководство по эксплуатации ПО в электронном формате	«Руководство по установке Платформы взаимодействия с конечными устройствами BI.ZONE EDR» v 1.32.0	B9f7e3f6e087b3024a0ad402ccddd370	Сторона разработчика ПО
	«Описание установки модуля алертов» версия от 27 ноября 2023 г.	efe2088b82d4c825f2e97613198e27e9	

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 По информации от разработчика ПО не поддерживает работу с активным режимом ЗПС. Испытания проводились при отключенном режиме ЗПС.

3.5 Внедрение ЭЦП в ELF/PE32-файлы выполняется некорректно, в связи с чем ПО не может функционировать с активным режимом ЗПС.

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.

4 Результаты испытаний

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

4.2 В ходе выполнения компонента ПО «BI.ZONE EDR Agent» в среде с ядрами 5.4.0-162-generic и 5.4.0-54-generic в /var/log/messages наблюдается однократное сообщение General Protection Fault, с другими ядрами такое поведение не было выявлено. Кроме записи в журнале последствий ошибки выявлено не было, ПО и ОС функционировали исправно, не наблюдалось отклонений от нормы.

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:

Умрихин А. В. – начальник отдела разработки инструментов выявления и реагирования на инциденты кибербезопасности ООО «БИЗон»;

Волков М. Н. – руководитель группы тестирования отдела разработки инструментов выявления и реагирования на инциденты кибербезопасности ООО «БИЗон».

ООО «БИЗон»

начальник отдела разработки инструментов выявления и реагирования на инциденты кибербезопасности

(подпись)

Умрихин А. В.

(фамилия, инициалы)

Приложение 1 к Протоколу № 22246/2024

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	5.4.0-54-hardened	5.4.0-162-generic	5.4.0-162-hardened	5.10.190-1-generic	5.10.190-1-hardened	5.15.0-83-generic	5.15.0-83-hardened	5.15.0-83-lowlatency	6.1.50-1-generic
1.	Установка ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
2.	Запуск, остановка выполнения ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
3.	Эксплуатация минимальной базовой функциональности ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
4.	Функционирование ПО в условиях низкого уровня целостности механизма МКЦ ОС	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
5.	Функционирование ПО в условиях ненулевого уровня конфиденциальности механизма МРД ОС	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно
6.	Отсутствие нарушений требований подраздела 17.3 «Руководство по КСЗ Ч. 1»	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
7.	Соответствие объектов ФС ОС дистрибутиву ОС при эксплуатации ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
8.	Удаление ПО	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно
9.	Функционирование ПО в условиях включённого механизма ЗПС ОС	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно	Неуспешно
10.	Отсутствие нарушений требований подраздела 17.2 «Руководство по КСЗ Ч. 1»	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно	Успешно

Приложение 2 к Протоколу № 22246/2024

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

2 Установка ПО:

2.1 выполнить действия:

развернуть ПО в соответствии с документами "Руководство по установке Платформы взаимодействия с конечными устройствами BI.ZONE EDR" и "Описание установки модуля алертов" Внимание! Компонент Relay развернуть на отдельном стенде с уникальным hostname

3 Удаление ПО:

3.1 выполнить действия:

произвести удаление ПО в соответствии с документами "Руководство по установке Платформы взаимодействия с конечными устройствами BI.ZONE EDR" и "Описание установки модуля алертов"

/ Ширинкин А.В./

Приложение 3 к Протоколу № 22246/2024

Перечень используемых сокращений

«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);

ДВиС – дирекция внедрения и сопровождения;

ЗПС – замкнутая программная среда;

КСЗ – комплекс средств защиты;

МКЦ – мандатный контроль целостности;

МРД – мандатное управление доступом;

ОС – операционная система;

ПО – программное обеспечение «BI.ZONE EDR Server» версии 1.32.0.