ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION»

РУСБ.10152-02

Руководство по КСЗ. Часть 2

Оперативное обновление 4.7.3

Бюллетень № 2022-1121SE47

Листов 9

2022

АННОТАЦИЯ

В настоящем руководстве приводятся изменения в документ РУСБ.10152-02 97 01-2 «Операционная система специального назначения «Astra Linux Special Edition». Руководство по КСЗ. Часть 2» из комплектности изделия РУСБ.10152-02 «Операционная система специального назначения «Astra Linux Special Edition» (далее по тексту — ОС), которые необходимо учитывать при проверке и тестировании комплекса средств защиты из состава ОС с установленным оперативным обновлением согласно бюллетеню № 2022-1121SE47.

Руководство предназначено для администраторов безопасности.

СОДЕРЖАНИЕ

1. Общие сведения 4
2. Перечень изменений 5
2.1. Пункт «1.1.5. Модуль тестирования механизма мандатного управления доступом при сетевых взаимодействиях» 5
2.2. Пункт «1.1.7. Модуль тестирования механизма очистки памяти внешних носителей» 5
2.3. Пункт «1.1.10. Модуль тестирования механизма мандатного контроля целостности» 5
2.4. Пункт «1.1.11. Модуль тестирования механизма управления метками безопасности» 5
2.5. Пункт «1.1.12. Модуль тестирования механизма фильтрации списка содержимого каталогов» 5
2.6. Пункт «1.1.13. Модуль тестирования механизма преобразования меток безопасности» 6
2.7. Пункт «1.2.38. mac-triggers-plperl, mac-triggers-plperlu, mac-triggers-plpgsql, mac-triggers-plpythonu, mac-triggers-pltcl, mac-triggers-pltclu» 6
2.8. Пункт «1.2.55. mac-declarative-part» 6
2.9. Пункт «1.2.56. mac-files» 6
2.10. Пункт «1.2.57. mac-replication-logical» 6
2.11. Пункт <1.2.58. <misc-memory-wiping» 7
2.12. Пункт «1.2.59. misc-notify» 7
2.13. Раздел «8. Проверка контроля подключения съемных машинных носителей информации и сопоставления пользователя с устройством» 7
2.14. Подраздел «9.2. Регистрация событий при работе с БД» 7
2.15. Раздел «11. Проверка работы механизма контроля целостности» 9

1. ОБЩИЕ СВЕДЕНИЯ

В настоящем руководстве приведены изменения в документ РУСБ.10152-02 97 01-2: измененные разделы, подразделы и пункты документа.

При проверке и тестировании комплекса средств защиты ОС с установленным оперативным обновлением согласно бюллетеню № 2022-1121SE47 рекомендуется руководствоваться документом РУСБ.10152-02 97 01-2 совместно с настоящим руководством.

2. ПЕРЕЧЕНЬ ИЗМЕНЕНИЙ

2.1. Пункт «1.1.5. Модуль тестирования механизма мандатного управления доступом при сетевых взаимодействиях»

В пункте 1.1.5 первый абзац изложить в редакции:

Реализован в виде тестов `tcpip_mac.sh` и `tcpip6_mac.sh` для версий протокола IPv4 и IPv6, соответственно.

2.2. Пункт «1.1.7. Модуль тестирования механизма очистки памяти внешних носителей»

В пункте 1.1.7 перечень поддерживаемых ФС дополнить файловой системой xfs.

2.3. Пункт «1.1.10. Модуль тестирования механизма мандатного контроля целостности»

Ввести новый пункт 1.1.10 в редакции:

1.1.10. Модуль тестирования механизма мандатного контроля целостности

Реализован в виде теста `mictest.sh`. Осуществляет следующие проверки:

1) разграничение доступа к файлам в соответствии с правилами МКЦ;
2) функционирование привилегии `PARSEC_CAP_IGNMACINT`;
3) ограничение отправки сигналов между процессами;
4) изменение уровня целостности;
5) функционирование метки целостности на юнитах systemd.

2.4. Пункт «1.1.11. Модуль тестирования механизма управления метками безопасности»

Ввести новый пункт 1.1.11 в редакции:

1.1.11. Модуль тестирования механизма управления метками безопасности

Реализован в виде теста `chlbl.sh`. Осуществляет проверки установки/снятия меток безопасности объектов в зависимости от:

1) типа объекта;
2) наличия привилегии суперпользователя `root`;
3) наличия привилегии `PARSEC_CAP_CHMAC`;
4) состояния МКЦ в системе (включено/выключено).

2.5. Пункт «1.1.12. Модуль тестирования механизма фильтрации списка содержимого каталогов»

Ввести новый пункт 1.1.12 в редакции:

1.1.12. Модуль тестирования механизма фильтрации списка содержимого каталогов

Реализован в виде теста `iterate_dir.sh`. Проверка фильтрации списка содержимого каталогов для объектов ФС ext4/xfs, имеющих ненулевую классификационную метку.

2.6. Пункт «1.1.13. Модуль тестирования механизма преобразования меток безопасности»

Ввести новый пункт 1.1.13 в редакции:

1.1.13. Модуль тестирования механизма преобразования меток безопасности

Реализован в виде теста `pdpl_test.sh`. Проверяет корректность преобразования меток безопасности из формата, в котором они хранятся на диске (в расширенных атрибутах файлов), в формат внутреннего представления.

2.7. Пункт «1.2.38. mac-triggers-plperl, mac-triggers-plperlu, mac-triggers-plpgsql, mac-triggers-plpythonu, mac-triggers-pltcl, mac-triggers-pltclu»

Изменить заголовок пункта 1.2.38:

1.2.38. mac-triggers-perl, mac-triggers-perlu, mac-triggers-pgsql, mac-triggers-pythonu, mac-triggers-tcl, mac-triggers-tclu

2.8. Пункт «1.2.55. mac-declarative-part»

Ввести новый пункт 1.2.55 в редакции:

1.2.55. mac-declarative-part

Проверка механизма мандатного управления доступом при декларативном секционировании заключается в создании таблицы с зависимыми от нее таблицами и изменении метки на родительской таблице. При этом проверяется наследование мандатной метки, признаков `CCR` и `MACS` родительской таблицы на дочерних таблицах при всех операциях изменения над родительской таблицей.

2.9. Пункт «1.2.56. mac-files»

Ввести новый пункт 1.2.56 в редакции:

Проверка установки мандатных атрибутов на файлы базы данных. При этом проверяется соответствие мандатных атрибутов объекта базы данных и всех файлов, принадлежащих данному объекту в файловой системе.

2.10. Пункт «1.2.57. mac-replication-logical»

Ввести новый пункт 1.2.57 в редакции:

Проверка мандатного управления доступом при логической репликации. При этом проверяются соблюдение правил разграничения доступа для объектов баз данных при взаимодействии двух серверов с помощью механизмов логической репликации.

2.11. Пункт <1.2.58. <misc-memory-wiping»

Ввести новый пункт 1.2.58 в редакции:

Проверка механизмов очистки памяти заключается в добавлении, изменении и удалении данных в таблице и самой таблицы. При этом проверяется очистка данных из файлов при их изменении или удалении из таблицы.

2.12. Пункт «1.2.59. misc-notify»

Ввести новый пункт 1.2.59 в редакции:

Проверка работы механизмов уведомлений с сообщениями. При этом проверяется невозможность несанкционированной передачи информации между уровнями.

2.13. Раздел «8. Проверка контроля подключения съемных машинных носителей информации и сопоставления пользователя с устройством»

В разделе 8 пункт 6) перечисления изложить в редакции:

6) добавить строку, предоставляющую пользователям право монтировать ФС подключенного USB-носителя:

```
/dev/sdc /mnt auto rw,user,noauto 0 0
```

Пункт 13) перечисления изложить в редакции:

13) смонтировать USB-носитель командой:

```
mount /mnt
```

2.14. Подраздел «9.2. Регистрация событий при работе с БД»

Подраздел 9.2 изложить в редакции:

9.2. Регистрация событий при работе с БД

Тестирование системы регистрации событий (аудита) СУБД PostgreSQL проводится в полуавтоматическом режиме. Тестированию подвергается требование к регистрации событий и фиксируемой в сообщениях аудита информации, а также к наличию средств выборочного ознакомления с информацией.

При выполнении тестирования (см. 2.2) генерируются следующие виды событий:

- использование механизма идентификации и аутентификации;
- попытки доступа;
- действия выделенных пользователей;
- запрос на доступ к защищаемому ресурсу;
- создание и удаление объекта;
- действия по изменению ПРД.

Для просмотра сообщений аудита СУБД необходимо:

1) войти в систему от имени администратора;

2) запустить окно терминала;

3) выполнить команду:

```
sudo ausearch -x postgres -i | more
```

Пример

Сообщение аудита, выданное СУБД PostgreSQL

```
type=PROCTITLE msg=audit(07.12.2021 11:49:01.438:13375) : proctitle=postgres:
     11/setest: postgres template1 [local] startup
type=SYSCALL msg=audit(07.12.2021 11:49:01.438:13375) : arch=x86_64
     syscall=write success=yes exit=94 a0=0x1f a1=0x1dd1410 a2=0x5e a3=0x0
     items=0 ppid=10726 pid=10760 auid=unset uid=postgres gid=postgres
     euid=postgres suid=postgres fsuid=postgres egid=postgres sgid=postgres
     fsgid=postgres tty=(none) ses=unset comm=postgres
     exe=/usr/lib/postgresql/11/bin/postgres subj=0:63:0:0 key=(null)
----
type=USER_AVC msg=audit(07.12.2021 11:49:01.438:13376) : user_parsec=success
     eid=257 msg0="SUBJECT" msg1="[local]" msg2="template1" msg3="postgres"
     msg4=" " msg5="postgres" msg6=" " msg7=":SQL:DROP USER u_0_01;"
     ppid=10726 pid=10760 auid=unset uid=postgres gid=postgres euid=postgres
     suid=postgres fsuid=postgres egid=postgres sgid=postgres fsgid=postgres
     tty=(none) ses=unset comm=postgres
     exe=/usr/lib/postgresql/11/bin/postgres subj=0:63:0:0
```

Из записи можно получить следующую информацию:

- успешность осуществления события (`success=yes` или `success=no`);
- тип события (`CONNECT`, `DISCONNECT`, `SUBJECT`, `RIGHTS` и т. д.);
- хост, с которого отправлен клиентский запрос (в приведенном примере `[local]`, что соответствует `localhost`);
- имя кластера, с которым работают (`setest`);
- имя БД, с которой работают (`template1`);
- имя авторизованного пользователя (`postgres`).

Описание остальных полей в записи:

- `type` — тип записи;
- `msg=audit` — запись времени события и его уникальный идентификационный номер
- `arch` — запись об архитектуре процессора;
- `syscall` — тип систем вызова;
- `success` — результат обработки вызова (успешно или нет);

- exit — значение выполнения, возвращенное системным вызовом;
- a0, a1, a2, a3 — четыре аргумента, закодированные в шестнадцатеричный формат, зависят от системного вызова;
- ppid — идентификационный номер родительского процесса;
- pid — идентификационный номер процесса;
- auid — идентификационный номер пользователя аудита;
- uid — имя пользователя, который вызвал процесс;
- gid — группа пользователя, который вызвал процесс;
- euid — имя действующего пользователя, который вызвал процесс;
- suid — имя пользователя, установленного во время выполнения;
- fsuid — имя пользователя файловой системы;
- egid — имя действующей группы пользователя, который вызвал процесс;
- sgid — имя группы пользователя, установленного во время выполнения;
- fsgid — имя группы пользователя файловой системы;
- tty — номер терминала, с которого вызван анализируемый процесс;
- ses — идентификационный номер сессии, в которой вызван анализируемый процесс;
- comm — название команды, из которой был вызван процесс;
- exe — путь до исполняемого файла, который вызвал анализируемый процесс;
- subj — контекст безопасности анализируемого процесса.

При проведении тестирования возможно настроить генерацию сообщений аудита PostgreSQL в интерактивном режиме, для этого в терминале от имени администратора выполнить команду:

```
watch -n 1  'ausearch -x postgres -i | tail'
```

При дальнейшей передаче SQL-команд в СУБД все сообщения аудита от СУБД PostgreSQL будут выводиться в терминал с интервалом равным одной секунде.

2.15. Раздел «11. Проверка работы механизма контроля целостности»

В разделе 11 пункт 6) перечисления изложить в редакции:

6) произвести намеренные изменения в ФС:

```
sudo -s
echo asdf >> /sbin/blkid
chmod 700 /sbin/sysctl
```