Средство защиты информации Secret Net LSP
Комментарии к версии 1.12

Документ содержит описание новых возможностей СЗИ Secret Net LSP (далее – Secret Net LSP) версии 1.12, а также особенностей и ограничений, которые необходимо учитывать при эксплуатации Secret Net LSP.

Оглавление

1. Комплект поставки

1.1. Размещение файлов на установочном диске

Каталог	Содержимое
\Setup\	Дистрибутивы
\Documentation\	Комплект документации
\Tools\	Вспомогательные утилиты, программы для установки и настройки ПО

2. Изменения и новые возможности

2.1. Версия 1.12

1. Доработан механизм контроля целостности (КЦ): расписание запуска КЦ, поддержка полного контроля над объектами, поддержка КЦ в реальном времени.

2. Добавлена возможность проверки запуска демонов и плагинов Secret Net LSP во время функционального контроля при старте системы.

3. Реализовано затирание файлов hugetlbfs через nmap.

4. Добавлена возможность проверки системы на работоспособность при включении жесткого режима замкнутой программной среды.

5. Реализована инициализация настроек из backUp при установке.

6. Реализован выбор реакции системы на обнаружение проблем при самотестировании или КЦ системы защиты.

7. Работа Secret Net LSP поддерживается в среде следующих операционных систем (ОС):

- Альт 8 СП (версия ядра 5.10.110-alt0.c9f.2, DE: MATE);
- Альт Рабочая Станция 9.2 (версия ядра 5.10.118-un-def-alt1, DE: MATE);
- Альт Сервер 9.2 (версия ядра 5.10.118-un-def-alt1, DE: MATE);
- Альт Рабочая Станция 10 (версия ядра 5.10.82-std-def-alt1, DE: MATE);
- Альт Сервер 10 (версия ядра 5.10.82-std-def-alt1, DE: MATE);
- Альт К 10 (версия ядра 5.15.37-un-def-alt1, DE: MATE);
- Ред ОС 7.3 (версия ядра 5.15.35-1.el7.x86_64, DE: MATE);
- Astra Linux Common Edition 2.12.44 (версия ядра 5.10.0-1038.40 generic/hardned, 5.4.0-71 generic/hardned, 4.15.3-141 generic/hardned, DE: FLY);
- Astra Linux Special Edition 1.7 (версия ядра 5.10.0-1045 generic/hardned, 5.4.0-81 generic/hardned, DE: FLY) и обновления № 2022-№ 0318SE17MD, № 2022-0407SE17MD;
- CentOS 7.9 (версия ядра 3.10.0-1160.66.1.el7.x86_64, DE: GNOME);
- CentOS 8.5 (версия ядра 4.18.0-348.7.1.el8_5.x86_64, DE: GNOME);
- Debian 11.3 (версия ядра 5.10.0-13-amd64, DE: GNOME);
- Oracle Linux 8.6 (версия ядра 4.18.0-372.9.1.el8.x86_64, 5.4.17-2136.307.3.4.el8uek.x86_64);
- Red Hat Enterprise Linux 7.9 (версия ядра 3.10.0-1160.66.1.el7.x86_64, DE: GNOME);
- Red Hat Enterprise Linux 8.5 (версия ядра 4.18.0-348.7.1.el8_5.x86_64, DE: GNOME);
- Red Hat Enterprise Linux 8.6 (версия ядра 4.18.0-372.9.1.el8.x86_64, DE: GNOME);
- SUSE Linux Enterprise Server 12 SP5 (версия ядра 4.12.14-120-default);
- SUSE Linux Enterprise Server 15 SP3 (версия ядра 5.3.18-57-default);
- Ubuntu 18.04 (версия ядра 5.4.134-19-generic, DE: GNOME);
- Ubuntu 18.04.6 (версия ядра 5.4.0-110-generic, DE: GNOME);
- Ubuntu 20.04.3 (версия ядра 5.10.65+yc0.406, 5.11.0-27-generic, DE: GNOME);
- Ubuntu 20.04.4 (версия ядра 5.13.0-41-generic, DE: GNOME);
- Ubuntu 22.04 (версия ядра 5.15.0-30-generic, DE: GNOME).

3. Особенности работы и ограничения

- ОС Debian, Ubuntu. При использовании механизмов ЗПС и МЭ рекомендуется отключить Wayland. При включенном Wayland также могут наблюдаться проблемы при отображении статуса лицензии при входе в систему. Для отключения необходимо в конфигурационном файле /etc/gdm3/daemon.conf задать параметр WaylandEnable=false.

- ОС Astra Linux CE 2.12, SE 1.7. В Secret Net LSP проявляются следующие особенности при работе с идентификаторами:
  - идентификация пользователя осуществляется только при вводе имени пользователя;
  - недоступна возможность блокировки при извлечении идентификатора.

- ОС Astra Linux CE 2.12, SE 1.7. Выключение подсистемы затирания информации происходит после перезагрузки компьютера.

- ОС Astra Linux CE 2.12, SE 1.7. Отсутствует техническая возможность менять пароль при входе пользователя через GUI.

- ОС Astra Linux CE 2.12, SE 1.7. Чтобы редактировать правила ЗПС Secret Net LSP через утилиту snaecctl при работе в CLI, нужно установить высокий уровень целостности для пользователя. Иначе правила будут применяться только после перезагрузки (или после рестарта сервиса).

- ОС Astra Linux CE 2.12, SE 1.7. После включения жесткого режима работы ЗПС Secret Net LSP блокирует процессы, запущенные учетной записью root.

- ОС Альт Рабочая станция 9. Из-за конфликта с пакетом OpenCT не работает идентификатор Rutoken S.

Существуют два способа решения проблемы.

1 способ. Удаление пакета OpenCT.

$ sudo rpm –e openct

Внимание! Также в системе не должен быть установлен пакет pcsc-lite-openct. Если пакет установлен, то его необходимо удалить.

2 способ. Удаление записей об идентификаторе в конфигурационном файле openct.conf.

С помощью текстового редактора в файле /etc/openct.conf необходимо изменить строки, относящиеся к Rutoken S, добавив символ # в начало строки. Например:

usb:0a89/0020, # Aktiv Rutoken S

usb:0a89/0012, # Aktiv uaToken S

- ОС Альт 8 СП. Вход в систему после предъявления идентификатора выполняется автоматически без запроса пароля, а для разблокирования экрана потребуется ввести пароль с клавиатуры.

- ОС Альт 8 СП. После установки Secret Net LSP, МЭ и лицензии. Если включить политику МЭ и затем создать любое правило, то выйдет ошибка, так как в системе не создан файл для хранения правил, что является ошибкой.

Если создать файл вручную, используя команду, то проблема будет решена:

mkdir touch /opt/snlsp-firewall/etc/suricata/rules/

touch /opt/snlsp-firewall/etc/suricata/rules/cfg.rules

- ОС РЕД ОС 7.3 Муром. В Secret Net LSP недоступна возможность включения политики "Уведомлять о последнем входе в систему" (политика last_log).

- ОС CentOS 7.x. Для корректного подключения к СБ необходимо использовать протокол NTLMv1. Это связано с особенностями ОС.

- ОС CentOS 7.x. При вводе в домен через sssd необходимо дополнительно установить пакет samba-winbind-modules (является зависимостью пакета samba-winbind), если не установлен, для корректной работы входа доменных пользователей.

- ОС CentOS 7.x, 8.x, РЕД ОС 7.3 Муром. Контроль доступа для системного диска не поддерживается, так как доступ к системному диску на этих дистрибутивах идет через виртуальное устройство.

- Secret Net LSP для работы сетевого взаимодействия имеет зависимость от пакета curl. При включении сетевого взаимодействия в Secret Net LSP может наблюдаться ошибка "OMS сервер не найден".

Диагностика: в логе /opt/secretnet/var/log/trace/snnetwork0.log отображается ошибка "CURL ERROR: end of task transmitting".

Решение: выполнить обновление пакета и библиотек curl до версии 7.68 или выше.

Если обновление не помогло:

  - для DEB-based систем необходимо в конфигурации openssl изменить параметр на CipherString = DEFAULT@SECLEVEL=1
  - для RPM-based систем необходимо выполнить команду:
    sudo update-crypto-policies –set LEGACY

- Для получения почтовых сообщений для администратора требуется установить postfix. При установке Secret Net LSP при установке зависимостей postfix рекомендуется устанавливать значения по умолчанию.
- Отсутствует возможность удаления устройств в Secret Net LSP с СБ SNS. Удаление устройства доступно только локально в Secret Net LSP.
- При установке межсетевого экрана доступ по протоколу ipv6 может быть ограничен.
- Опции межсетевого экрана, проверяющие содержимое сетевого пакета, работают только с незашифрованым трафиком.
- В Secret Net LSP не поддерживается работа с именами пользователей, в которых содержатся кириллические символы. В режиме усиленной аутентификации доменных пользователей имя (логин) при входе в систему должно содержать только латинские символы. Если в имени присутствуют символы кириллицы, параметру "Усиленная аутентификация" следует установить значение "Выключено".
- Для получения информации о доменном пользователе Secret Net LSP используется атрибут пользователя userPrincipalName из Active Directory. Для корректной работы с доменными пользователями у них должен присутствовать данный атрибут.
- При работе с идентификатором Jacarta ГОСТ необходимо предварительно выполнить его инициализацию и установить персональный идентификационный номер с помощью ПО Аладдин jcadmin.
- Для доменного пользователя игнорируется чтение закрытого ключа с идентификатора.
- Если в домене используется большое количество учетных записей/групп, то рекомендуется отключить перечисление для пользователей/групп в системных сервисах, отвечающих за взаимодействие с доменом (SSSD/samba).

Для SSSD –в конфигурационном файле /etc/sssd/sssd.conf необходимо изменить значение:
enumerate = false
Для samba – в конфигурационном файле /etc/samba/smb.conf необходимо изменить значения:
winbind enum users = no
winbind enum groups = no

- Пакет openssh-server, необходимый для удаленного подключения от СБ к агенту управления, убран из обязательных зависимостей.
- Пакеты cups, sendmail убраны из обязательных зависимостей. cups используется для контроля печати, sendmail\postfix для отправки почтовых сообщений администратору.
- При попытке включить подсистему печати без включенной политики cups, система выводит ошибку (кроме CentOS 7.x, 8.x, RHEL 8.x, Oracle Linux 8.x).

4. Сведения о совместимости с другим ПО

В разделе содержатся сведения о совместимости Secret Net LSP версии 1.12 со сторонними программными средствами при совместном функционировании.

1. Реализована совместимость Secret Net LSP со следующими продуктами ООО "Код Безопасности":
   - СЗИ Secret Net Studio 8.6, 8.8;
   - ПАК "Соболь" 3.0.6, 3.0.9, 3.1, 3.2, 4.3, 4.4;
   - СКЗИ "Континент-АП" Linux 3.7.5, 4.0.
2. Реализована совместимость Secret Net LSP со следующим ПО:
   - Мой Офис 1.28.0.4;
   - Kaspersky Endpoint Security 11.2.0.4528 для Linux;
   - Dr.Web Desktop Security Suite версии 11.1.

ООО "КОД БЕЗОПАСНОСТИ"

Почтовый адрес:	115127, Москва, а/я 66
Телефон:	(495) 982-30-20
Email:	info@securitycode.ru
Web:	https://www.securitycode.ru