ASR5x00, Выполняющий резервное копирование .chassisid файл (ID шасси) на StarOS, освобождает 20 и Выше

Содержание

Введение

Этот документ описывает, как выполнить резервное копирование**, .chassisidfile** (ID шасси) на StarOS освобождает 20 и выше.

Общие сведения

Ключ шасси используется, чтобы зашифровать и дешифровать зашифрованные пароли в файле конфигурации. Если два или больше шасси настроены с тем же значением параметра шасси, зашифрованные пароли могут быть дешифрованы любым из шасси, совместно использующих то же значение параметра шасси. Как заключение к этому, данное значение параметра шасси не может дешифровать пароли, которые были зашифрованы с другим значением параметра шасси.

Ключ шасси используется для генерации ID шасси, который сохранен в файле и используется в качестве главного ключа для защиты уязвимых данных (таких как пароли и тайны) в файлах конфигурации

Для выпуска 15.0 и выше, ID шасси является хэшем SHA256 ключа шасси. Ключ шасси может быть установлен пользователями через команду CLI или через Быстрого Мастера настройки. Если ID шасси не существует, локальный MAC - адрес используется для генерации ID шасси.

Для выпуска 19.2 и выше, пользователь должен явно установить ключ шасси через Быстрого Мастера настройки или команду CLI. Если это - "not set", ID шасси по умолчанию с помощью локального MAC - адреса генерируется. В отсутствие ключа шасси (и следовательно ID шасси), уязвимые данные не появляются в сохраненном файле конфигурации.

ID шасси является **хэшем SHA256 (закодированный в формате base36) введенного ключа шасси пользователя плюс 32-байтовое безопасное случайное число.** Это гарантирует, что ключ шасси и ID шасси имеют 32-байтовую энтропию для ключевой безопасности.

Если ID шасси не является доступным шифрованием, и расшифровка для уязвимых данных в файлах конфигурации не работают.

Проблема: Недостаточный для выполнения резервное копирование значения параметра шасси для выполнения для одинаковой конфигурации на том же узле.

Из-за изменения в поведении начиная с выпуска 19.2, не достаточно больше выполнить резервное копирование значение параметра шасси, чтобы быть в состоянии выполнить одинаковую конфигурацию на том же узле.

Кроме того, из-за случайного 32-байтового номера, подключенного к настроенному ключу шасси, всегда существуют другие ID шасси, генерируемые на основе тех же ключей шасси.

Это - причина, почему **шасси** команды CLI **keycheck** скрыто теперь начиная с нее, всегда возвращаются отрицательный, даже если введен тот же старый ключ.

Чтобы быть в состоянии восстановить машину StarOS с сохраненной конфигурации (когда, например все содержание **/ флэш-накопителя** было потеряно), это - requred для создания копии **.chassisid** (где StarOS хранит ID шасси),

ID шасси сохранен в **/flash/.chassisid** файле на жестком диске StarOS. Наилегчайший метод выполнения резервное копирование этого файла должен передать его через некоторый файл trasfer протокол к серверу резервного копирования:

Поскольку вы видите**, что .chassisid файл** является скрытым, и с более новыми версиями не возможно сделать операции управления файлами со скрытыми файлами. Например, эта ошибка отображена с выпуском 20.0.1:

```
[local]sim-lte# copy /flash/.chassisid /flash/backup
Failure: source is not valid.
[local]sim-lte#
```

Или:

```
[local]sim-lte# show file url /flash/.chassisid
Failure: file is not valid.
```

Решение

Существует все еще способ обратиться к этому файлу с помощью этой процедуры:

Шаг 1. Гарантируйте**, что .chassisid** файл присутствует в**/flash/.chassisid**.

```
[local]sim-lte# dir /flash/.chassisid
-rw-rw-r--   1 root    root          53 Jun 23 10:59 /flash/.chassisid
8      /flash/.chassisid
Filesystem          1k-blocks     Used Available Use% Mounted on
/var/run/storage/flash/part1  523992   192112   331880 37% /mnt/user/.auto/onboard/flash
```

Шаг 2. Вход в систему в скрытый режим.

```
[local]sim-lte# cli test-commands
Password:
Warning: Test commands enables internal testing and debugging commands
USE OF THIS MODE MAY CAUSE SIGNIFICANT SERVICE INTERRUPTION
[local]sim-lte#
```

> **Примечание:** Если нет никакого скрытого настроенного пароля режима nable, настройте его с этим:

```
[local]sim-lte# cli test-commands
Password:
Warning: Test commands enables internal testing and debugging commands
USE OF THIS MODE MAY CAUSE SIGNIFICANT SERVICE INTERRUPTION
[local]sim-lte#
```

Шаг 3. Запустите оболочку отладки.

```
[local]sim-lte# debug shell
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
Cisco Systems QvPC-SI Intelligent Mobile Gateway
[No authentication; running a login shell]
```

Шаг 4. . Перемещение в **/ флэше - каталоге**. Проверьте, ли файл там.

```
sim-lte:ssi#
sim-lte:ssi# ls
bin cdrom1 hd-raid param rmm1 tmp usr
boot dev include pcmcia1 sbin usb1 var
boot1 etc lib proc sftp usb2 vr
boot2 flash mnt records sys usb3
sim-lte:ssi#
sim-lte:ssi# cd flash
sim-lte:ssi# ls -a
. ldlinux.sys restart_file_cntr.txt
.. module.sys sftp
.chassisid patch staros.bin
crashlog2 persistdump syslinux.ban
crsh2 rc.local syslinux.cfg
```

Шаг 5. . Скопируйте скрытый файл к нескрытому.

```
sim-lte:ssi# cp .chassisid chassisid.backup
sim-lte:ssi#
sim-lte:ssi#
sim-lte:ssi# ls
chassisid.backup patch staros.bin
crashlog2 persistdump syslinux.ban
crsh2 rc.local syslinux.cfg
ldlinux.sys restart_file_cntr.txt
module.sys sftp
```

Шаг 6. Выйдите из оболочки отладки. Должна существовать возможность передать резервный файл, созданный без любых проблем.

```
sim-lte:ssi# exit
Connection closed by foreign host.
[local]sim-lte#
[local]sim-lte# copy /flash/chassisid.backup /flash/chasisid.backup2
************************************************************************
Transferred 53 bytes in 0.003 seconds (17.3 KB/sec)
```

```
[local]sim-lte#
[local]sim-lte#
[local]sim-lte# show file url /flash/chassisid.backup
1ke03dqfdb9dw3kds7vdslvuls3jnop8yj41qyh29w7urhno4ya6
```