Рекомендации по обеспечению безопасности применения СКЗИ в условиях наличия уязвимостей прикладного и системного ПО

Применимость документа

Рекомендации данного документа применимы к следующим исполнениям СКЗИ «С-Терра VPN» версии 4.3:

«6-1», «6-3», «6-5».

Рекомендации по обеспечению безопасности

Для обеспечения безопасности применения СКЗИ в условиях наличия уязвимостей прикладного и системного ПО следует выполнять следующие требования.

1. Рекомендуется обеспечить защиту от локального нарушителя при помощи организационно-технических мер.

   Данная мера позволяет нейтрализовать следующие уязвимости:

   CVE-2019-11599, CVE-2023-37453.

2. Управление устройством по SSH должно быть разрешено только при наличии доверенного канала связи (защищенного при помощи СКЗИ).

   Данная мера позволяет нейтрализовать следующие уязвимости:

   CVE-2017-9078, CVE-2018-15599, CVE-2016-7406, CVE-2016-7407.

3. Не рекомендуется исполнять ПО, а также получать и открывать файлы, полученные из недоверенных источников.

   Данная мера позволяет нейтрализовать следующие уязвимости:

   CVE-2019-1010023, CVE-2017-15412, CVE-2018-1061, CVE-2018-14647, CVE-2018-0494, CVE-2019-5953, CVE-2020-8492, CVE-2016-3189, CVE-2017-13089, CVE-2019-16935, CVE-2019-18348, CVE-2017-13090, CVE-2018-1060, CVE-2018-9251, CVE-2020-1752, CVE-2019-1010220, CVE-2020-7982, CVE-2017-10661, CVE-2021-28831, CVE-2021-37566, CVE-2021-37560, CVE-2021-35055, CVE-2021-37584, CVE-2021-37563, CVE-2021-37561.

4. Рекомендуется использовать IPsec туннель/доверенный канал до серверов DNS, NTP, SNMP, CIFS и для доступа к web-интерфейсу, web-порталам.

   Данная мера позволяет нейтрализовать следующие уязвимости:

CVE-2017-14495, CVE-2017-14496, CVE-2019-14513, CVE-2017-14491, CVE-2016-6301, CVE-2018-18066, CVE-2018-1066, CVE-2020-10871, CVE-2018-19630, CVE-2019-5101, CVE-2019-5102.

5. Не рекомендуется использовать файловую систему debugfs.

   Данная мера позволяет нейтрализовать уязвимость:

   CVE-2019-19770

6. Рекомендуется использовать SNMP-клиент, не изменяя формат вывода.

   Данная мера позволяет нейтрализовать уязвимость:

   CVE-2014-3565

7. Не рекомендуется использовать UPnP в продукте.

   Данная мера позволяет нейтрализовать уязвимость:

   CVE-2020-12695

8. Рекомендуется применить следующие команды по установке безопасных параметров в ОС (Внимание: уменьшение порогов может повлиять на обработку больших UDP пакетов):

```
sysctl -w net.ipv4.ipfrag_low_thresh=196608
sysctl -w net.ipv4.ipfrag_high_thresh=262144
```

   Данная мера позволяет нейтрализовать уязвимость:

   CVE-2018-5391

9. Рекомендуется устанавливать CRL только из доверенных источников.

   Данная мера позволяет нейтрализовать уязвимость:

   CVE-2023-0286

10. Рекомендуется запускать на Продукте только доверенные приложения. Рекомендуется не использовать скрипты для автоматической генерации регулярных выражений.

    Данная мера позволяет нейтрализовать уязвимость:

    CVE-2021-35942. Уязвимость исправлена точечным патчем в образе BIM43_2022_06_01.

11. Рекомендуется использовать wget только для получения данных из доверенных источников. Не рекомендуется использование в keepalived подсистемы отличной от VRRP. В качестве метода аутентификации рекомендуется использовать только auth_type PASS.

    Данная мера позволяет нейтрализовать уязвимости:

    CVE-2021-3712. Уязвимость исправлена точечным патчем в образе BIM43_2022_06_01.

Отдельные уязвимости, отсутствие которых проверено

1. Уязвимость *CVE-2022-0847* относится к версиям ядра, не используемым в Продукте, отсутствие проверено практически.
2. Для устранения уязвимостей *CVE-2019-12272, CVE-2018-20679* разработан и применен патч.
3. Уязвимости *CVE-2019-15945, CVE-2019-15946, CVE-2019-16746, CVE-2019-17133, CVE-2017-18017* устранены внесением патча.
4. Уязвимость *CVE-2020-28951* устранена патчем без обновления версии пакета `uci`.
5. Уязвимость *CVE-2021-3326* устранена патчем без обновления версии пакета `libc`.