

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, включая контроль доступа и АПМДЗ.

Данная мера позволяет нейтрализовать уязвимость:

CVE-2019-11599

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.

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 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, CVE-2020-1563.

10. Не рекомендуется использовать скрипты для автоматической генерации регулярных выражений.

Данная мера позволяет нейтрализовать уязвимость:

CVE-2021-35942

Отдельные уязвимости, отсутствие которых проверено

1. Уязвимость *CVE-2022-0847* относится к версиям ядра, не используемым в Продукте, отсутствие проверено практически.