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:

«3-1», «3-3», «3-5», «5-1», «5-3», «5-5».

Рекомендации по обеспечению безопасности

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

Внимание! Версия образа – значение переменной `CVSTAG`, указанное в файле `/etc/image_version`.

---

1. Рекомендуется использовать встроенные в СКЗИ механизмы безопасности для обеспечения доверенного канала.

   Данная мера позволяет нейтрализовать следующие уязвимости:

   CVE-2017-7507, CVE-2021-20232, CVE-2018-10845, CVE-2021-33560, CVE-2017-7869, CVE-2021-20231, CVE-2021-20305, CVE-2017-0379, CVE-2020-24659, CVE-2019-3829, CVE-2018-10844.

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-2019-3861, CVE-2020-14145, CVE-2019-3863, CVE-2019-3862, CVE-2018-20685, CVE-2019-3858, CVE-2019-3857, CVE-2019-3860, CVE-2019-6109, CVE-2020-15778, CVE-2019-17498, CVE-2019-3856, CVE-2018-15473, CVE-2019-3855, CVE-2018-15919, CVE-2019-3859, CVE-2019-6111, CVE-2019-6110, CVE-2019-13115, CVE-2021-40528 (уязвимость исправлена в пакете `libgcrypt20` версии `1.7.6-2+deb9u4`, версия образа BIM43_2023_07_20), *CVE-2022-0778* (уязвимость исправлена в пакете `libssl` версии `1.1.0l-1~deb9u5`, версия образа BIM43_2023_07_20), *CVE-2021-36368*, *CVE-2023-48795, CVE-2023-51385.*

3. Не рекомендуется получать файлы из недоверенных источников, при необходимости проверять их антивирусной программой.

Не рекомендуется загружать файлы на Шлюз непосредственно с не контролируемых администратором СКЗИ серверов.

Не рекомендуется открывать файлы, полученные из недоверенных источников, в том числе не рекомендуется распаковывать на Шлюзе архивы, созданные не администратором СКЗИ.

При использовании файлов, полученных из недоверенных источников, рекомендуется убеждаться, что файл соответствует назначению - сертификат относится к нужному узлу, политика безопасности содержит необходимые правила и т.п.

Данная мера позволяет нейтрализовать следующие уязвимости:

CVE-2019-8907, CVE-2019-9072, CVE-2017-6508, CVE-2018-14618, CVE-2017-18258, CVE-2017-14107, CVE-2017-12459, CVE-2019-9071, CVE-2018-14567, CVE-2017-13732, CVE-2018-14647, CVE-2017-7225, CVE-2017-8421, CVE-2017-9048, CVE-2018-14048, CVE-2017-9044, CVE-2017-7375, CVE-2019-17595, CVE-2019-8906, CVE-2017-16879, CVE-2017-12133, CVE-2019-10160, CVE-2019-9074, CVE-2019-19333, CVE-2018-9251, CVE-2019-14250, CVE-2019-1010023, CVE-2017-7468, CVE-2019-20367, CVE-2018-16842, CVE-2017-7299, CVE-2019-12972, CVE-2019-20398, CVE-2017-9756, CVE-2019-9633, CVE-2017-12456, CVE-2017-12451, CVE-2019-13232, CVE-2017-15412, CVE-2018-19517, CVE-2019-1010204, CVE-2017-9747, CVE-2016-9318, CVE-2017-7614, CVE-2018-6798, CVE-2017-13734, CVE-2018-1000122, CVE-2017-9743, CVE-2017-1000099, CVE-2017-16931, CVE-2017-9050, CVE-2017-17522, CVE-2018-1000005, CVE-2019-9070, CVE-2018-13785, CVE-2018-18520, CVE-2019-16168, CVE-2017-9754, CVE-2017-6965, CVE-2017-6969, CVE-2018-13410, CVE-2016-2073, CVE-2017-9745, CVE-2017-6966, CVE-2018-19217, CVE-2017-12453, CVE-2017-13730, CVE-2017-9042, CVE-2017-12458, CVE-2017-9955, CVE-2021-20193, CVE-2019-9077, CVE-2019-9073, CVE-2017-13729, CVE-2017-1000257, CVE-2017-5969, CVE-2016-9598, CVE-2017-12450, CVE-2018-20671, CVE-2019-5953, CVE-2019-20393, CVE-2018-19932, CVE-2019-12290, CVE-2019-17594, CVE-2017-9040, CVE-2017-7210, CVE-2017-7376, CVE-2019-14444, CVE-2019-17450, CVE-2016-2037, CVE-2017-9049, CVE-2017-9749, CVE-2018-20843, CVE-2017-12457, CVE-2018-1000121, CVE-2017-16997, CVE-2017-12883, CVE-2020-14382, CVE-2019-11360, CVE-2019-9923, CVE-2017-9750, CVE-2017-9748, CVE-2018-0500, CVE-2017-12454, CVE-2019-9076, CVE-2016-9596, CVE-2017-5130, CVE-2019-6129, CVE-2017-13090, CVE-2017-9753, CVE-2017-9752, CVE-2017-12858, CVE-2017-9746, CVE-2017-12652, CVE-2017-9778, CVE-2018-18384, CVE-2017-9751, CVE-2017-9742, CVE-2019-16167, CVE-2018-1000301, CVE-2017-12449, CVE-2019-16935, CVE-2019-8905, CVE-2016-5131, CVE-2017-9744, CVE-2018-14404, CVE-2017-1000100, CVE-2019-15601, CVE-2017-9047, CVE-2019-20396, CVE-2017-9043, CVE-2017-9233, CVE-2019-5481, CVE-2019-17371, CVE-2018-1000858, CVE-2017-9039, CVE-2017-9041, CVE-2017-7223, CVE-2017-12452, CVE-2017-12588, CVE-2019-10654, CVE-2017-7224, CVE-2018-14550, CVE-2019-8904, CVE-2018-1000120, CVE-2016-4483, CVE-2018-19416, CVE-2019-20394, CVE-2019-15903, CVE-2019-19334, CVE-2018-6797, CVE-2019-20392, CVE-2018-1000007, CVE-2018-1000300, CVE-2019-7317, CVE-2017-13089, CVE-2017-9755, CVE-2020-26541, CVE-2018-20969, CVE-2017-8872, CVE-2017-12448, CVE-2018-10360, CVE-2017-9038, CVE-2017-13733, CVE-2019-13638, CVE-2017-7209, CVE-2019-5435, CVE-2017-2629, CVE-2017-8817, CVE-2020-8492, CVE-2019-20397, CVE-2019-1010180, CVE-2017-9954, CVE-2017-1000254, CVE-2019-5482, CVE-2017-13731, CVE-2017-13728, CVE-2018-0494, CVE-2017-16932, CVE-2019-20391, CVE-2019-17451, CVE-2019-20395, CVE-2017-12455, CVE-2016-6321, CVE-2018-1000035, CVE-2017-10661, CVE-2021-4217, CVE-2022-0529, CVE-2022-0530, CVE-2021-3697, CVE-2022-48303, CVE-2023-27534, CVE-2023-4735, CVE-2024-2398, CVE-2023-4751, CVE-2023-4734, CVE-2023-4781, CVE-2023-4750, CVE-2023-

4733, CVE-2023-39804, CVE-2023-4738, CVE-2024-32487, CVE-2023-45918, CVE-2023-4752, CVE-2023-5535, CVE-2023-7216, CVE-2024-43802, CVE-2024-43374, CVE-2024-43790, CVE-2024-39929, CVE-2024-41957.

4. Рекомендуется использовать IPsec туннель/доверенный канал до серверов DHCP, DNS, NTP, SNMP, FTP, syslog, BGP, OSPF, RIP.

   Данная мера позволяет нейтрализовать следующие уязвимости:

   CVE-2018-5732, CVE-2019-8936, CVE-2018-7182, CVE-2019-11331, CVE-2018-7183, CVE-2018-7184, CVE-2017-12132, CVE-2017-15908, CVE-2017-9217, CVE-2018-1000140, CVE-2018-16881, CVE-2019-17040, CVE-2020-11868, CVE-2020-13817, CVE-2018-12327, CVE-2017-15906, CVE-2017-9445, CVE-2018-18066, CVE-2022-24805, CVE-2022-24806, CVE-2022-24807, CVE-2022-24808, CVE-2022-24809, CVE-2022-24810, CVE-2022-44792, CVE-2022-44793, CVE-2023-26551, CVE-2023-26552, CVE-2023-26553, CVE-2023-26554, CVE-2023-26555, CVE-2022-24903, CVE-2022-37032, CVE-2023-38408.

5. Работа с Zabbix должна осуществляться только в доверенной сети.

   Данная мера позволяет нейтрализовать следующие уязвимости:

   CVE-2019-17382, CVE-2019-15132, CVE-2021-46088, CVE-2024-36460, CVE-2024-36467, CVE-2024-36461, CVE-2024-42327, CVE-2024-36466, CVE-2024-22116.

6. При работе с Zabbix-сервером серверное приложение должно быть обновлено до версии 6.4.18rc1 или выше при использовании версии 6.4.x, до версии 7.0.2rc1 или выше при использовании версии 7.0.x, до 7.2.0alpha1 или выше при использовании версии 7.2.x.

   Данная мера позволяет нейтрализовать следующие уязвимости:

   CVE-2024-36460, CVE-2024-36467, CVE-2024-36461, CVE-2024-42327, CVE-2024-36466, CVE-2024-22116.

7. При использовании exim и msmtp для отправки электронных сообщений рекомендуется пользоваться доверенными SMTP-серверами.

   Данная мера позволяет нейтрализовать следующие уязвимости:

   CVE-2019-15846, CVE-2021-27216, CVE-2020-28025, CVE-2020-28008, CVE-2020-28013, CVE-2020-28022, CVE-2020-28020, CVE-2020-28012, CVE-2020-28011, CVE-2020-28023, CVE-2020-28026, CVE-2020-28016, CVE-2020-28019, CVE-2020-28015, CVE-2020-12783, CVE-2020-28018, CVE-2017-16943, CVE-2020-28014, CVE-2020-28007, CVE-2020-28024, CVE-2018-6789, CVE-2019-13917, CVE-2019-10149, CVE-2019-16928, CVE-2017-16944, CVE-2020-28010, CVE-2020-28017, CVE-2020-28009, CVE-2019-8337, CVE-2022-37452, CVE-2023-42116, CVE-2023-42117, CVE-2023-42119, CVE-2023-51766.

8. Не рекомендуется использовать файловую систему debugfs.

   Данная мера позволяет нейтрализовать уязвимость:

   CVE-2019-19770

9. Рекомендуется ограничить доступ к порту UDP 111 при помощи встроенного межсетевого экрана (МЭ).

   Данная мера позволяет нейтрализовать уязвимость:

   CVE-2017-8804

10. 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 уязвимости:

    CVE-2018-5390, CVE-2018-5391

11. Рекомендуется использовать `auth_login` из состава СКЗИ для аутентификации в системе.

    Данная мера позволяет нейтрализовать уязвимости:

    CVE-2017-1000082, CVE-2018-20839

12. Не рекомендуется разрабатывать скрипты автоматизации с использованием Python и dbus.

    Данная мера позволяет нейтрализовать уязвимости:

    CVE-2022-22824, CVE-2022-23990, CVE-2022-22823, CVE-2022-22822, CVE-2022-23852.

    Уязвимости исправлены в пакете `libexpat1` версии `2.2.0-2+deb9u4`, версия образа BIM43_2023_07_20.

13. Рекомендуется использовать `curl, wget и ntp` 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`. Рекомендуется использовать доступ по ssh, iperf, tcpdump и snmp только внутри IPsec канала.

    Данная мера позволяет нейтрализовать уязвимости:

    CVE-2021-3712, CVE-2020-1968, CVE-2022-32221, CVE-2023-27533.

    Уязвимости исправлены в пакете `libssl` версии `1.0.2u-1~deb9u6` и `libssl 1.1.0l-1~deb9u4`, версия образа BIM43_2023_07_20.

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

    Данная мера позволяет нейтрализовать уязвимость:

    CVE-2021-35942 (уязвимость исправлена в пакете `libc` версии `2.24-11+deb9u4st1`, версия образа BIM43_2023_07_20).

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

    Данная мера позволяет нейтрализовать: *CVE-2023-47233, CVE-2024-36894, CVE-2023-52886, CVE-2023-52670, CVE-2021-47476, CVE-2024-26652, CVE-2023-4693.*

16. Не рекомендуется использовать кодировку ISO-2022-CN-EXT. Такая кодировка по умолчанию не используется продуктом, и не предлагается пользователю в штатных сценариях работы.

    Данная мера позволяет нейтрализовать: *CVE-2024-2961.*

Отдельные уязвимости, отсутствие которых проверено

1. Уязвимость *CVE-2022-0847* относится к версиям ядра, не используемым в Продукте, отсутствие проверено практически.
2. Уязвимости *CVE-2019-15165, CVE-2019-15163, CVE-2019-15162, CVE-2019-15164, CVE-2019-15161* устранены патчем в пакет `libpcap0.8` версии 1.8.1-3 в версии образа BIM43_2023_07_20.
3. Уязвимость *CVE-2019-19965* устранена внесением патча в образ версии BIM43_2023_07_20.
4. Уязвимость *CVE-2021-41617* не может проявляться. Администратор системы имеет полный доступ и не является нарушителем. Непривилегированный пользователь не может эксплуатировать данную уязвимость.