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

Применимость документа

Документ применим 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 с в условиях наличия уязвимостей прикладного и системного ПО следует выполнять следующие требования.

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

Данная мера позволяет нейтрализовать следующие уязвимости:

CVE-2019-13115, CVE-2018-15473, CVE-2018-15919, CVE-2018-20685, CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3858, CVE-2019-3859, CVE-2019-3860, CVE-2019-3861, CVE-2019-3862, CVE-2019-3863, CVE-2019-6109, CVE-2019-6110, CVE-2019-6111, CVE-2019-17498.

2. Не рекомендуется исполнять ПО, полученное из недоверенных источников, а также получать и открывать файлы из недоверенных источников.

Данная мера позволяет нейтрализовать следующие уязвимости:

CVE-2016-2037, CVE-2016-2073, CVE-2016-4483, CVE-2017-1000099, CVE-2017-12133, CVE-2017-12448, CVE-2017-12449, CVE-2017-12450, CVE-2017-12451, CVE-2017-12452, CVE-2017-12453, CVE-2017-12454, CVE-2017-12455, CVE-2017-12456, CVE-2017-12457, CVE-2017-12458, CVE-2017-12459, CVE-2017-12588, CVE-2017-12652, CVE-2017-12858, CVE-2017-12883, CVE-2017-13728, CVE-2017-13729, CVE-2017-13730, CVE-2017-13731, CVE-2017-13732, CVE-2017-13733, CVE-2017-13734, CVE-2017-14107, CVE-2017-16879, CVE-2017-16931, CVE-2017-16932, CVE-2017-16997, CVE-2017-17522, CVE-2017-18258, CVE-2017-5969, CVE-2017-6965, CVE-2017-6966, CVE-2017-6969, CVE-2017-7209, CVE-2017-7210, CVE-2017-7223, CVE-2017-7224, CVE-2017-7225, CVE-2017-7299, CVE-2017-7375, CVE-2017-7376, CVE-2017-7614, CVE-2017-8421, CVE-2017-8872, CVE-2017-9038, CVE-2017-9039, CVE-2017-9040, CVE-2017-9041, CVE-2017-9042, CVE-2017-9043, CVE-2017-9044, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050, CVE-2017-9233, CVE-2017-9742, CVE-2017-9743, CVE-2017-9744, CVE-2017-9745, CVE-2017-9746, CVE-2017-9747, CVE-2017-9748, CVE-2017-9749, CVE-2017-9750, CVE-2017-9751, CVE-2017-9752, CVE-2017-9753, CVE-2017-9754, CVE-2017-9755, CVE-2017-9756, CVE-2017-9778, CVE-2017-9954, CVE-2017-9955, CVE-2018-0500, CVE-2018-1000035, CVE-2018-1000300, CVE-2018-1000858, CVE-2018-10360, CVE-2018-13410, CVE-2018-13785, CVE-2018-14048, CVE-2018-14404, CVE-2018-14550, CVE-2018-14567, CVE-2018-18384, CVE-2018-18520, CVE-2018-19217, CVE-2018-19416, CVE-2018-19517, CVE-2018-19932, CVE-2018-20671, CVE-2018-20843, CVE-2018-20969, CVE-2018-9251, CVE-2019-13232, CVE-2019-15903, CVE-2019-16167, CVE-2019-17371, CVE-2019-5435, CVE-2019-5481, CVE-2019-5482, CVE-2019-

5953, CVE-2019-7317, CVE-2019-8904, CVE-2019-8905, CVE-2019-8906, CVE-2019-8907, CVE-2019-9923, CVE-2016-6321, CVE-2017-1000100, CVE-2017-1000254, CVE-2017-1000257, CVE-2017-13089, CVE-2017-13090, CVE-2017-2629, CVE-2017-6508, CVE-2017-7468, CVE-2017-8817, CVE-2018-0494, CVE-2018-1000005, CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2018-1000301, CVE-2018-14618, CVE-2018-14647, CVE-2018-16842, CVE-2018-6797, CVE-2018-6798, CVE-2019-1010023, CVE-2019-1010180, CVE-2019-1010204, CVE-2019-10160, CVE-2019-10654, CVE-2019-11360, CVE-2019-13638, CVE-2019-12290, CVE-2019-12972, CVE-2019-14250, CVE-2019-14444, CVE-2019-16935, CVE-2019-17450, CVE-2019-17451, CVE-2019-17594, CVE-2019-17595, CVE-2019-6129, CVE-2019-9070, CVE-2019-9071, CVE-2019-9072, CVE-2019-9073, CVE-2019-9074, CVE-2019-9076, CVE-2019-9077, CVE-2020-8492, CVE-2019-15601, CVE-2019-16168, CVE-2019-19333, CVE-2019-19334, CVE-2019-20367, CVE-2019-20391, CVE-2019-20392, CVE-2019-20393, CVE-2019-20394, CVE-2019-20395, CVE-2019-20396, CVE-2019-20397, CVE-2019-20398, CVE-2019-9633, CVE-2017-10661.

3. Рекомендуется подключаться к DHCP-серверу по доверенному каналу/сегменту сети.

Данная мера позволяет нейтрализовать уязвимость CVE-2018-5732.

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

Данная мера позволяет нейтрализовать следующие уязвимости:

CVE-2019-15132, CVE-2019-17382.

5. При использовании exim4 и msmtp для отправки электронных сообщений рекомендуется пользоваться доверенными SMTP-серверами.

Данная мера позволяет нейтрализовать следующие уязвимости:

CVE-2018-5733, CVE-2017-16944, CVE-2019-13917, CVE-2019-15846, CVE-2017-16943, CVE-2019-10149, CVE-2018-6789, CVE-2019-16928, CVE-2019-8337.

6. Рекомендуется использовать IPsec туннель/доверенный канал до серверов DNS, NTP, SNMP, FTP, syslog.

Данная мера позволяет нейтрализовать следующие уязвимости:

CVE-2017-9445, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, CVE-2019-11331, CVE-2019-8936, CVE-2018-18066, CVE-2017-12132, CVE-2017-15908, CVE-2017-9217, CVE-2017-15906, CVE-2018-12327, CVE-2018-1000140, CVE-2018-16881, CVE-2019-17040.

7. Не рекомендуется использовать rsyslog в продукте для обработки AIX и cisco логов

Данная мера позволяет нейтрализовать следующие уязвимости:

CVE-2019-17041, CVE-2019-17042.

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 МЭ.

Данная мера позволяет нейтрализовать уязвимость CVE-2017-8804.

10. Рекомендуется не монтировать удаленные директории через недоверенные сегменты сети. Рекомендуется не монтировать удаленные директории с недоверенных узлов.

Данная мера позволяет нейтрализовать уязвимость CVE-2018-1049.

11. Рекомендуется не использовать NFS для обмена данными через недоверенные сегменты сети. Рекомендуется не использовать NFS для обмена данными с недоверенным узлом.

Данная мера позволяет нейтрализовать уязвимости CVE-2017-8797 и CVE-2018-16871.

12. Рекомендуется использовать технологию IPMI только через доверенные сегменты сети.

Данная мера позволяет нейтрализовать уязвимости CVE-2019-9003, CVE-2019-19046.