НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2023-07-07.1 | 7 июля 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-20185	Cisco Nexus 9000 Series Switches in ACI Mode	Сетевой	OSI	2023-07-07	✓
2	Высокая	CVE-2023-22633	FortiNAC	Сетевой	DoS	2023-06-13	✓
3	Высокая	CVE-2023-33672	Tenda AC8	Сетевой	ACE	2023-06-02	✓
4	Высокая	CVE-2023-28000	FortiADC CLI	Локальный	ACE	2023-06-13	✓
5	Высокая	CVE-2022-43953	Fortinet FortiOS	Локальный	ACE	2023-06-13	✓
6	Высокая	CVE-2022-43949	FortiSIEM	Сетевой	OSI	2023-06-13	✓
7	Высокая	CVE-2023-33533	Netgear	Сетевой	ACE	2023-06-06	✗
8	Высокая	CVE-2023-33530	Tenda G103	Сетевой	ACE	2023-06-06	✗
9	Высокая	CVE-2023-33538	TP-Link TL-WR940N V2/V4 TL-WR841N V8/V10 TL-WR740N V1/V2	Сетевой	ACE	2023-06-07	✗
10	Высокая	CVE-2023-33536	TP-Link TL-WR940N V2/V4 TL-WR841N V8/V10 TL-WR740N V1/V2	Сетевой	DoS	2023-06-07	✗
11	Высокая	CVE-2022-39946	FortiNAC	Сетевой	ACE	2023-06-13	✓
12	Высокая	CVE-2023-22639	Fortinet FortiOS	Локальный	PE	2023-06-13	✓

13	Высокая	CVE-2023-26210	FortiADC	Локальный	PE	2023-06-13	✓
14	Критическая	CVE-2023-33299	Fortinet FortiNAC	Сетевой	ACE	2023-06-23	✗
15	Высокая	CVE-2022-41327	Fortinet FortiOS	Локальный	OSI	2023-06-13	✓
16	Критическая	CVE-2023-26204	FortiSIEM	Сетевой	ACE	2023-06-13	✓
17	Критическая	CVE-2023-31569	TOTOLINK X5000R	Сетевой	ACE	2023-06-06	✓
18	Критическая	CVE-2023-33556	TOTOLink A7100RU	Сетевой	ACE	2023-06-07	✓
19	Критическая	CVE-2023-33675	Tenda AC8	Сетевой	ACE	2023-06-12	✓
20	Критическая	CVE-2023-33673	Tenda AC8	Сетевой	ACE	2023-06-12	✓
21	Критическая	CVE-2023-33671	Tenda AC8	Сетевой	ACE	2023-06-12	✓
22	Критическая	CVE-2023-33670	Tenda AC8	Сетевой	ACE	2023-06-12	✓
23	Критическая	CVE-2023-33669	Tenda AC8	Сетевой	ACE	2023-06-12	✓
24	Критическая	CVE-2023-34566	Tenda AC10	Сетевой	ACE	2023-06-08	✓
25	Критическая	CVE-2023-33532	Netgear R6250	Сетевой	PE	2023-06-06	✓

1

Краткое описание: Получение конфиденциальной информации в Cisco Nexus 9000 Series Switches in ACI Mode

Идентификатор уязвимости: CVE-2023-20185

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Cisco Nexus 9000 Series Switches in ACI Mode: 14.0 - 14.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.4 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-07 / 2023-07-07

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-aci-cloudsec-enc-Vs5Wn2sX
- https://bdu.fstec.ru/vul/2023-03583

2

Краткое описание: Отказ в обслуживании в FortiNAC

Идентификатор уязвимости: CVE-2023-22633

Идентификатор программной ошибки: Не определено

Уязвимый продукт: FortiNAC: до 9.4.1, до 9.2.6, до 9.1.8, до 8.8.0, 8.7.0 все версии, FortiNAC-F 7.2.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-13 / 2023-06-16

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-22633

3

Краткое описание: Выполнение произвольного кода в Tenda AC8

Идентификатор уязвимости: CVE-2023-33672

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC8: V4.0-V16.03.34.06

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-02 / 2023-06-12

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-33672

4

Краткое описание: Выполнение произвольного кода в FortiADC CLI

Идентификатор уязвимости: CVE-2023-28000

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: FortiADC CLI: 7.1.0, 7.0.0 - 7.0.3, 6.2.0 - 6.2.4, 6.1 все версии, 6.0 все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-13 / 2023-06-20

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-28000
- https://bdu.fstec.ru/vul/2023-03505

5

Краткое описание: Выполнение произвольного кода в Fortinet FortiOS

Идентификатор уязвимости: CVE-2022-43953

Идентификатор программной ошибки: CWE-134 Использование форматной строки, контролируемой извне

Уязвимый продукт: Fortinet FortiOS:
версии 7.2.0–7.2.4,
7.0 все версии,
6.4 все версии,
6.2 все версии,
FortiProxy версии 7.2.0–7.2.1,
FortiProxy версии 7.0.0 до 7.0.7

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-13 / 2023-06-16

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2022-43953

6

Краткое описание: Получение конфиденциальной информации в FortiSIEM

Идентификатор уязвимости: CVE-2022-43949

Идентификатор программной ошибки: CWE-327 Использование скомпрометированного или ненадежного криптографического алгоритма

Уязвимый продукт: FortiSIEM: до 6.7.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-13 / 2023-06-17

Ссылки на источник:

- https://fortiguard.com/psirt/FG-IR-22-259
- https://bdu.fstec.ru/vul/2023-03353

7

Краткое описание: Выполнение произвольного кода в Netgear

Идентификатор уязвимости: CVE-2023-33533

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: Netgear:
D6220 with Firmware Version 1.0.0.80
D8500 with Firmware Version 1.0.3.60
R6700 with Firmware Version 1.0.2.26
R6900 with Firmware Version 1.0.2.26

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-06 / 2023-07-14

Ссылки на источник:

- https://github.com/D2y6p/CVE/blob/main/Netgear/CVE-2023-33533/Netgear_RCE.pdf
- https://bdu.fstec.ru/vul/2023-03192

8

Краткое описание: Выполнение произвольного кода в Tenda G103

Идентификатор уязвимости: CVE-2023-33530

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: Tenda G103: Gigabit GPON Terminal with firmware version V1.0.0.5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-06 / 2023-06-15

Ссылки на источник:

- https://github.com/D2y6p/CVE/blob/main/tenda/CVE-2023-33530/RCE2/tenda_G103_RCE_2.pdf
- https://bdu.fstec.ru/vul/2023-03195

9

Краткое описание: Выполнение произвольного кода в TP-Link TL-WR940N V2/V4 TL-WR841N V8/V10 TL-WR740N V1/V2

Идентификатор уязвимости: CVE-2023-33538

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: TP-Link TL-WR940N V2/V4
TL-WR841N V8/V10
TL-WR740N V1/V2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-07 / 2023-06-13

Ссылки на источник:

- https://github.com/a101e-IoTvul/iotvul/blob/main/tp-link/3/TL-WR940N_TL-WR841N_userRpm_WlanNetworkRpm_Command_Injection.md
- https://bdu.fstec.ru/vul/2023-03182

10

Краткое описание: Отказ в обслуживании в TP-Link TL-WR940N V2/V4 TL-WR841N V8/V10 TL-WR740N V1/V2

Идентификатор уязвимости: CVE-2023-33536

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: TP-Link TL-WR940N V2/V4
TL-WR841N V8/V10
TL-WR740N V1/V2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-07 / 2023-06-13

Ссылки на источник:

- https://github.com/a101e-IoTvul/iotvul/blob/main/tp-link/2/TL-WR940N_TL-WR841N_TL-WR740N_userRpm_WlanMacFilterRpm.md
- https://bdu.fstec.ru/vul/2023-03207

Краткое описание: Выполнение произвольного кода в FortiNAC

Идентификатор уязвимости: CVE-2022-39946

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: FortiNAC: 8.5.0 - 9.4.2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Выполнение произвольного кода

11 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.6 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-13 / 2023-06-13

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-22-332

12

Краткое описание: Повышение привилегий в Fortinet FortiOS

Идентификатор уязвимости: CVE-2023-22639

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Fortinet FortiOS: версии 7.2.0–7.2.3,
FortiOS: версии 7.0.0–7.0.10,
FortiOS: версии 6.4.0–6.4.12,
FortiOS: всех версий 6.2,
FortiOS: всех версий 6.0,
FortiProxy: версии 7.2.0–7.2.2,
FortiProxy: версии 7.0.0–7.0.8,
FortiProxy: всех версий 2.0,
FortiProxy: всех версий 1.2,
FortiProxy: всех версий 1.1,
FortiProxy: всех версий 1.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-13 / 2023-06-16

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-22639
- https://bdu.fstec.ru/vul/2023-03354

Краткое описание: Повышение привилегий в FortiADC

Идентификатор уязвимости: CVE-2023-26210

Идентификатор программной ошибки: CWE-78 Некорректная нейтрализация специальных элементов, используемых в системных командах (внедрение команд ОС)

Уязвимый продукт: FortiADC: 5.2.0 - 7.2.0
FortiADC Manager: 5.2.0 - 7.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Повышение привилегий

13

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-13 / 2023-06-13

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-076
- https://bdu.fstec.ru/vul/2023-03506

14

Краткое описание: Выполнение произвольного кода в Fortinet FortiNAC

Идентификатор уязвимости: CVE-2023-33299

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Fortinet FortiNAC: 8.5.0 - 8.5.4, 8.6.0 - 8.6.5, 8.7.0 - 8.7.6, 8.8.0 - 8.8.11, 9.1.0 - 9.1.9,9.2.0 - 9.2.7

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-23 / 2023-07-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-33299

Краткое описание: Получение конфиденциальной информации в Fortinet FortiOS

Идентификатор уязвимости: CVE-2022-41327

Идентификатор программной ошибки: CWE-319 Передача важных данных в незашифрованном виде

Уязвимый продукт: Fortinet FortiOS: 7.2.0–7.2.4, 7.0.0–7.0.8
FortiProxy: 7.2.0–7.2.1 и 7.0.0–7.0.8

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Получение конфиденциальной информации

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

15

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-13 / 2023-06-16

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2022-41327
- https://bdu.fstec.ru/vul/2023-03357

Краткое описание: Выполнение произвольного кода в FortiSIEM

Идентификатор уязвимости: CVE-2023-26204

Идентификатор программной ошибки: CWE-522 Недостаточно надежная защита учетных данных

Уязвимый продукт: FortiSIEM: 6.7 все версии, 6.6 все версии, 6.5 все версии, 6.4 все версии, 6.3 все версии, 6.2 все версии, 6.1 все версии, 5.4 все версии, 5.3 все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

16

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-13 / 2023-06-13

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-26204
- https://bdu.fstec.ru/vul/2023-03356

17

Краткое описание: Выполнение произвольного кода в TOTOLINK X5000R

Идентификатор уязвимости: CVE-2023-31569

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: TOTOLINK X5000R: V9.1.0cu.2350_B20230313

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-06 / 2023-06-12

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-31569

18

Краткое описание: Выполнение произвольного кода в TOTOLink A7100RU

Идентификатор уязвимости: CVE-2023-33556

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: TOTOLink A7100RU: V7.4cu.2313_B20191024

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-07 / 2023-06-13

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-33556

Краткое описание: Выполнение произвольного кода в Tenda AC8

Идентификатор уязвимости: CVE-2023-33675

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC8: V4.0-V16.03.34.06

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

19 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-12 / 2023-06-12

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-33675

Краткое описание: Выполнение произвольного кода в Tenda AC8

Идентификатор уязвимости: CVE-2023-33673

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC8: V4.0-V16.03.34.06

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

20

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-12 / 2023-06-12

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-33673

Краткое описание: Выполнение произвольного кода в Tenda AC8

Идентификатор уязвимости: CVE-2023-33671

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC8: V4.0-V16.03.34.06

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

21 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-12 / 2023-06-12

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-33671

Краткое описание: Выполнение произвольного кода в Tenda AC8

Идентификатор уязвимости: CVE-2023-33670

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC8: V4.0-V16.03.34.06

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

22

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-12 / 2023-06-12

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-33670

Краткое описание: Выполнение произвольного кода в Tenda AC8

Идентификатор уязвимости: CVE-2023-33669

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC8: V4.0-V16.03.34.06

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

23

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-12 / 2023-06-12

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-33669

Краткое описание: Выполнение произвольного кода в Tenda AC10

Идентификатор уязвимости: CVE-2023-34566

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda AC10: v4 US_AC10V4.0si_V16.03.10.13_cn

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

24

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-08 / 2023-06-14

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-34566

Краткое описание: Повышение привилегий в Netgear R6250

Идентификатор уязвимости: CVE-2023-33532

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: Netgear R6250: 1.0.4.48

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

25

Оценка CVSSv3: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-06 / 2023-06-12

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-33532
- https://bdu.fstec.ru/vul/2023-03194