НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-09-15.1 | 15 сентября 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-41375	Kostac PLC Programming Software	Локальный	ACE	2023-09-15	✓
2	Высокая	CVE-2023-41374	JTEKT ELECTRONICS Kostac PLC Programming Software	Локальный	ACE	2023-09-15	✓
3	Высокая	CVE-2023-39669	D-Link DIR-880	Сетевой	DoS	2023-08-17	✗
4	Высокая	CVE-2023-39829	Tenda A18	Сетевой	ACE	2023-08-14	✗
5	Высокая	CVE-2023-39828	Tenda A18	Сетевой	ACE	2023-08-14	✗
6	Критическая	CVE-2023-38940	Tenda routers	Сетевой	ACE	2023-08-07	✗
7	Критическая	CVE-2023-38933	Tenda routers	Сетевой	ACE	2023-08-07	✗
8	Критическая	CVE-2023-38937	Tenda routers	Сетевой	ACE	2023-08-07	✗
9	Критическая	CVE-2023-38936	Tenda routers	Сетевой	ACE	2023-08-07	✗
10	Критическая	CVE-2023-39666	D-Link DIR-842 Rev.A	Сетевой	ACE	2023-08-17	✗
11	Критическая	CVE-2023-39749	D-Link DAP-2660	Сетевой	DoS	2023-08-20	✗
12	Высокая	CVE-2023-4481	Juniper Junos OS	Сетевой	DoS	2023-08-29	✗

1

Краткое описание: Выполнение произвольного кода в Kostac PLC Programming Software

Идентификатор уязвимости: CVE-2023-41375

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Kostac PLC Programming Software: 1.6.11.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-15 / 2023-09-15

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU95282683/index.html

2

Краткое описание: Выполнение произвольного кода в JTEKT ELECTRONICS Kostac PLC Programming Software

Идентификатор уязвимости: CVE-2023-41374

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: JTEKT ELECTRONICS Kostac PLC Programming Software: 1.6.11.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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:N/UI:R/S:U/C:H/I:H/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-09-15 / 2023-09-15

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU95282683/index.html

3

Краткое описание: Отказ в обслуживании в D-Link DIR-880

Идентификатор уязвимости: CVE-2023-39669

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: D-Link DIR-880: A1_FW107WWb08

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Дата выявления / Дата обновления: 2023-08-17 / 2023-08-25

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-39669
- https://bdu.fstec.ru/vul/2023-04863

4

Краткое описание: Выполнение произвольного кода в Tenda A18

Идентификатор уязвимости: CVE-2023-39829

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda A18: V15.13.07.09

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Дата выявления / Дата обновления: 2023-08-14 / 2023-08-18

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-39829

5

Краткое описание: Выполнение произвольного кода в Tenda A18

Идентификатор уязвимости: CVE-2023-39828

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda A18: V15.13.07.09

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Дата выявления / Дата обновления: 2023-08-14 / 2023-09-18

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-39828

Краткое описание: Выполнение произвольного кода в Tenda routers

Идентификатор уязвимости: CVE-2023-38940

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda routers:
Tenda F1203: V2.0.1.6
Tenda FH1203: V2.0.1.6
Tenda FH1205: V2.0.0.7 (775)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

6

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

Дата выявления / Дата обновления: 2023-08-07 / 2023-08-09

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-38940

7

Краткое описание: Выполнение произвольного кода в Tenda routers

Идентификатор уязвимости: CVE-2023-38933

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda routers:
Tenda AC6: V2.0 V15.03.06.23
Tenda AC7: V1.0 V15.03.06.44
Tenda F1203: V2.0.1.6
Tenda AC5: V1.0 V15.03.06.28
Tenda FH1203: V2.0.1.6
Tenda AC9: V3.0 V15.03.06.42_multi
Tenda FH1205: V2.0.0.7 (775)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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

Дата выявления / Дата обновления: 2023-08-07 / 2023-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-38933
- https://bdu.fstec.ru/vul/2023-04556

8

Краткое описание: Выполнение произвольного кода в Tenda routers

Идентификатор уязвимости: CVE-2023-38937

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda routers:
Tenda AC10: V1.0 V15.03.06.23
Tenda AC1206: V15.03.06.23
Tenda AC8: v4 V16.03.34.06
Tenda AC6: V2.0 V15.03.06.23
Tenda AC7: V1.0 V15.03.06.44
Tenda AC5: V1.0 V15.03.06.28
Tenda AC9 V3.0 V15.03.06.28
Tenda AC9 V3.0 V15.03.06.42_multi
Tenda AC10 v4.0 V16.03.10.13

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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

Дата выявления / Дата обновления: 2023-08-07 / 2023-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-38937

Краткое описание: Выполнение произвольного кода в Tenda routers

Идентификатор уязвимости: CVE-2023-38936

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Tenda routers:
Tenda AC10: V1.0 V15.03.06.23
Tenda AC1206: V15.03.06.23
Tenda AC6: V2.0 V15.03.06.23
Tenda AC7: V1.0 V15.03.06.44
Tenda AC5: V1.0 V15.03.06.28
Tenda FH1203: V2.0.1.6
Tenda AC9: V3.0 V15.03.06.42_multi
Tenda FH1205: V2.0.0.7(775)

9

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

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

Дата выявления / Дата обновления: 2023-08-07 / 2023-08-10

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-38936
- https://bdu.fstec.ru/vul/2023-04558

Краткое описание: Выполнение произвольного кода в D-Link DIR-842 Rev.A

Идентификатор уязвимости: CVE-2023-39666

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: D-Link DIR-842 Rev.A: до 1-02_eu_multi_20151008

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

10

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

Дата выявления / Дата обновления: 2023-08-17 / 2023-08-25

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-39666
- https://bdu.fstec.ru/vul/2023-04860

Краткое описание: Отказ в обслуживании в D-Link DAP-2660

Идентификатор уязвимости: CVE-2023-39749

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: D-Link DAP-2660: до v1.13

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Отказ в обслуживании

11

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

Дата выявления / Дата обновления: 2023-08-20 / 2023-08-24

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-39749
- https://bdu.fstec.ru/vul/2023-04916

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2023-4481

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Juniper Junos OS: все версии
Junos OS Evolved: все версии

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Отказ в обслуживании

12

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

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

Дата выявления / Дата обновления: 2023-08-29 / 2023-08-29

Ссылки на источник:

- http://supportportal.juniper.net/s/article/2023-08-29-Out-of-Cycle-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-A-crafted-BGP-UPDATE-message-allows-a-remote-attacker-to-de-peer-reset-BGP-sessions-CVE-2023-4481
- https://bdu.fstec.ru/vul/2023-05091