НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-07-12.1 | 12 июля 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-33127	Visual Studio	Сетевой	PE	2023-07-12	✓
2	Высокая	CVE-2023-36867	Visual Studio Code - GitHub Pull Requests and Issues Extension	Локальный	ACE	2023-07-12	✓
3	Высокая	CVE-2023-35330	Windows	Сетевой	DoS	2023-07-12	✓
4	Высокая	CVE-2023-32038	Windows	Сетевой	ACE	2023-07-12	✓
5	Высокая	CVE-2023-35313	Windows	Локальный	ACE	2023-07-12	✓
6	Высокая	CVE-2023-33170	Ubuntu	Сетевой	ACE	2023-07-12	✓
7	Не определено	CVE-2023-37450	Apple Safari и macOS Ventura	Не определено	ACE	2023-07-11	✓
8	Не определено	CVE-2023-37450	WebKitGTK+	Не определено	ACE	2023-07-11	✗
9	Высокая	CVE-2023-36359	TP-Link TL-WR940N V4 TL-WR841N V8/V10 TL-WR940N V2/V3 TL-WR941ND V5/V6	Сетевой	DoS	2023-06-22	✓
10	Высокая	CVE-2023-36358	TP-Link TL-WR940N V2/V3/V4 TL-WR941ND V5/V6 TL-WR743ND V1 TL-WR841N V8	Сетевой	DoS	2023-06-22	✓

11	Высокая	CVE-2023-36357	TP-Link TL-WR940N V2/V4/V6 TL-WR841N V8/V10 TL-WR941ND V5	Сетевой	DoS	2023-06-22	✓
12	Высокая	CVE-2023-36356	TP-Link TL-WR940N V2/V4/V6 TL-WR841N V8 TL-WR941ND V5 TL-WR740N V1/V2	Сетевой	DoS	2023-06-22	✗
13	Высокая	CVE-2023-36354	TP-Link TL-WR940N V4 TL-WR841N V8/V10 TL-WR740N V1/V2 TL-WR940N V2/V3 TL-WR941ND V5/V6	Сетевой	DoS	2023-06-22	✓
14	Критическая	CVE-2023-34832	TP-Link Archer AX10(EU)_V1.2_230220	Сетевой	DoS	2023-06-16	✗
15	Критическая	CVE-2023-36355	TP-Link TL-WR940N V4	Сетевой	DoS	2023-06-22	✓
16	Критическая	CVE-2023-34563	netgear R6250 Firmware Version 1.0.4.48	Сетевой	DoS	2023-06-20	✗
17	Критическая	CVE-2023-26613	D-Link DIR-823G firmware version 1.02B05	Сетевой	ACE	2023-06-29	✗
18	Критическая	CVE-2023-26612	D-Link DIR-823G firmware version 1.02B05	Сетевой	DoS	2023-06-29	✗
19	Критическая	CVE-2023-26616	D-Link DIR-823G firmware version 1.02B05	Сетевой	DoS	2023-06-29	✗
20	Критическая	CVE-2023-27992	Zyxel NAS326 до V5.21, NAS540 до V5.2, NAS542 до V5.21	Сетевой	ACE	2023-06-19	✓

21	Высокая	CVE-2023-37202	Ubuntu	Сетевой	ACE	2023-07-11	✓
22	Высокая	CVE-2023-37201	Ubuntu	Сетевой	ACE	2023-07-11	✓
23	Высокая	CVE-2023-35940	GLPI	Сетевой	OSI	2023-07-10	✓
24	Критическая	CVE-2023-34416	Ubuntu	Сетевой	ACE	2023-07-11	✓
25	Высокая	CVE-2023-35924	GLPI	Сетевой	ACE	2023-07-10	✓
26	Высокая	CVE-2023-35939	GLPI	Сетевой	ACE	2023-07-10	✓
27	Критическая	CVE-2023-36664	Ubuntu	Сетевой	ACE	2023-07-10	✓
28	Высокая	CVE-2023-36808	GLPI	Сетевой	ACE	2023-07-10	✓
29	Критическая	CVE-2023-36934	MOVEit Transfer	Сетевой	ACE	2023-07-10	✓
30	Высокая	CVE-2023-24329	Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions	Сетевой	SB	2023-07-10	✓

Краткое описание: Повышение привилегий в Visual Studio

Идентификатор уязвимости: CVE-2023-33127

Идентификатор программной ошибки: CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)

Уязвимый продукт: Visual Studio: 2022 version 17.0 - 2022 version 17.6
.NET: 6.0.0 - 7.0.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

1 **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: 8.1 AV:N/AC:H/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: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-33127

2

Краткое описание: Выполнение произвольного кода в Visual Studio Code - GitHub Pull Requests and Issues Extension

Идентификатор уязвимости: CVE-2023-36867

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Visual Studio Code - GitHub Pull Requests and Issues Extension: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36867

3

Краткое описание: Отказ в обслуживании в Windows

Идентификатор уязвимости: CVE-2023-35330

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 22H2
Windows Server: 2008 R2 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

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: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35330

4

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-32038

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 22H2
Windows Server: 2008 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32038

5

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2023-35313

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Windows: 10 - 11 22H2
Windows Server: 2016 - 2022 20H2

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35313

6

Краткое описание: Выполнение произвольного кода в Ubuntu

Идентификатор уязвимости: CVE-2023-33170

Идентификатор программной ошибки: CWE-362 Одновременное использование общих ресурсов при выполнении кода без соответствующей синхронизации (состояние гонки)

Уязвимый продукт: Ubuntu: 22.04 - 23.04
dotnet-host-7.0 (Ubuntu package): до 7.0.109-0ubuntu1~23.04.1
dotnet-runtime-6.0 (Ubuntu package): до 6.0.120-0ubuntu1~23.04.1
dotnet-runtime-7.0 (Ubuntu package): до 7.0.109-0ubuntu1~23.04.1
dotnet7 (Ubuntu package): до 7.0.109-0ubuntu1~23.04.1
dotnet6 (Ubuntu package): до 6.0.120-0ubuntu1~23.04.1
dotnet-sdk-7.0 (Ubuntu package): до 7.0.109-0ubuntu1~23.04.1
dotnet-sdk-6.0 (Ubuntu package): до 6.0.120-0ubuntu1~23.04.1
aspnetcore-runtime-7.0 (Ubuntu package): до 7.0.109-0ubuntu1~23.04.1
dotnet-host (Ubuntu package): до 6.0.120-0ubuntu1~23.04.1
dotnet-hostfxr-6.0 (Ubuntu package): до 6.0.120-0ubuntu1~23.04.1
dotnet-hostfxr-7.0 (Ubuntu package): до 7.0.109-0ubuntu1~23.04.1
aspnetcore-runtime-6.0 (Ubuntu package): до 6.0.120-0ubuntu1~23.04.1

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

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: 8.1 AV:N/AC:H/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: 2023-07-12 / 2023-07-12

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6217-1

Краткое описание: Выполнение произвольного кода в Apple Safari и macOS Ventura

Идентификатор уязвимости: CVE-2023-37450

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Apple Safari и macOS Ventura:
macOS 13.0 22A380 - 13.4.1 22F82,
Apple Safari 16.0 - 16.5.1

Категория уязвимого продукта: Операционные системы Apple и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

7 **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: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-11 / 2023-07-11

Ссылки на источник:

- http://support.apple.com/en-us/HT213825
- http://support.apple.com/en-us/HT201224
- http://support.apple.com/en-us/HT213826

8

Краткое описание: Выполнение произвольного кода в WebKitGTK+

Идентификатор уязвимости: CVE-2023-37450

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: WebKitGTK+: все версии
WPE WebKit: все версии

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: Не определено

Вектор атаки: Не определено

Взаимодействие с пользователем: Не определено

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-11 / 2023-07-11

Ссылки на источник:

- http://support.apple.com/en-us/HT213823

9

Краткое описание: Отказ в обслуживании в TP-Link TL-WR940N V4 TL-WR841N V8/V10 TL-WR940N V2/V3 TL-WR941ND V5/V6

Идентификатор уязвимости: CVE-2023-36359

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

Уязвимый продукт: TP-Link TL-WR940N V4
TL-WR841N V8/V10
TL-WR940N V2/V3
TL-WR941ND V5/V6

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

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: 2023-06-22 / 2023-06-29

Ссылки на источник:

- https://github.com/a101e-IoTvul/iotvul/blob/main/tp-link/8/TP-Link%20TL-WR940N%20TL-WR841N%20TL-WR941ND%20wireless%20router%20userRpmQoSRuleListRpm%20buffer%20read%20out-of-bounds%20vulnerability.md

Краткое описание: Отказ в обслуживании в TP-Link TL-WR940N V2/V3/V4 TL-WR941ND V5/V6 TL-WR743ND V1 TL-WR841N V8

Идентификатор уязвимости: CVE-2023-36358

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

Уязвимый продукт: TP-Link TL-WR940N V2/V3/V4
TL-WR941ND V5/V6
TL-WR743ND V1
TL-WR841N V8

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

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: 7.7 AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-22 / 2023-06-30

Ссылки на источник:

- https://github.com/a101e-IoTvul/iotvul/blob/main/tp-link/6/TL-WR940N_WR941ND_WR743ND_WR841N_userRpm_AccessCtrlAccessTargetsRpm.md
- https://bdu.fstec.ru/vul/2023-03599

11

Краткое описание: Отказ в обслуживании в TP-Link TL-WR940N V2/V4/V6 TL-WR841N V8/V10 TL-WR941ND V5

Идентификатор уязвимости: CVE-2023-36357

Идентификатор программной ошибки: Не определено

Уязвимый продукт: TP-Link TL-WR940N V2/V4/V6
TL-WR841N V8/V10
TL-WR941ND V5

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

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: 7.7 AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-22 / 2023-06-30

Ссылки на источник:

- https://github.com/a101e-IoTvul/iotvul/blob/main/tp-link/5/TL-WR941ND_TL-WR940N_TL-WR841N_userRpm_LocalManageControlRpm.md

Краткое описание: Отказ в обслуживании в TP-Link TL-WR940N V2/V4/V6 TL-WR841N V8 TL-WR941ND V5 TL-WR740N V1/V2

Идентификатор уязвимости: CVE-2023-36356

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: TP-Link TL-WR940N V2/V4/V6
TL-WR841N V8
TL-WR941ND V5
TL-WR740N V1/V2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Отказ в обслуживании

12 **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: 7.7 AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-22 / 2023-06-30

Ссылки на источник:

- https://github.com/a101e-IoTvul/iotvul/blob/main/tp-link/4/TL-WR941ND_TL-WR940N_TL-WR740N_userRpm_VirtualServerRpm.md
- https://bdu.fstec.ru/vul/2023-03611

Краткое описание: Отказ в обслуживании в TP-Link TL-WR940N V4 TL-WR841N V8/V10 TL-WR740N V1/V2 TL-WR940N V2/V3 TL-WR941ND V5/V6

Идентификатор уязвимости: CVE-2023-36354

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

Уязвимый продукт: TP-Link TL-WR940N V4
TL-WR841N V8/V10
TL-WR740N V1/V2
TL-WR940N V2/V3
TL-WR941ND V5/V6

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

13 **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: 2023-06-22 / 2023-06-29

Ссылки на источник:

- https://github.com/a101e-IoTvul/iotvul/blob/main/tp-link/7/TL-WR940N_TL-WR841N_TL-WR740N_TL-WR941ND_userRpm_AccessCtrlTimeSchedRpm.md

Краткое описание: Отказ в обслуживании в TP-Link Archer AX10(EU)_V1.2_230220

Идентификатор уязвимости: CVE-2023-34832

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

Уязвимый продукт: TP-Link Archer AX10(EU)_V1.2_230220

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

14 **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: 2023-06-16 / 2023-06-23

Ссылки на источник:

- https://gist.github.com/jhacker91/2026e080a42514255e758d64b465d1d5
- http://archer.com
- http://tp-link.com
- http://packetstormsecurity.com/files/172989/TP-Link-Archer-AX10-EU-_V1.2_230220-Buffer-Overflow.html
- https://bdu.fstec.ru/vul/2023-03518

Краткое описание: Отказ в обслуживании в TP-Link TL-WR940N V4

Идентификатор уязвимости: CVE-2023-36355

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

Уязвимый продукт: TP-Link TL-WR940N V4

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

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.

15

Оценка CVSSv3: 9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-06-22 / 2023-07-04

Ссылки на источник:

- https://github.com/a101e-IoTvul/iotvul/blob/main/tp-link/9/TP-Link%20TL-WR940N%20wireless%20router%20userRpmWanDynamicIpV6CfgRpm%20buffer%20write%20out-of-bounds%20vulnerability.md
- http://packetstormsecurity.com/files/173294/TP-Link-TL-WR940N-4-Buffer-Overflow.html

16

Краткое описание: Отказ в обслуживании в netgear R6250 Firmware Version 1.0.4.48

Идентификатор уязвимости: CVE-2023-34563

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

Уязвимый продукт: netgear R6250 Firmware Version 1.0.4.48

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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: 2023-06-20 / 2023-06-28

Ссылки на источник:

- https://www.netgear.com/about/security/
- https://github.com/D2y6p/CVE/blob/main/Netgear/CVE-2023-34563/EN.md
- https://bdu.fstec.ru/vul/2023-03580

17

Краткое описание: Выполнение произвольного кода в D-Link DIR-823G firmware version 1.02B05

Идентификатор уязвимости: CVE-2023-26613

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

Уязвимый продукт: D-Link DIR-823G firmware version 1.02B05

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: 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: 2023-06-29 / 2023-07-06

Ссылки на источник:

- https://www.dlink.com/en/security-bulletin/
- https://github.com/726232111/VulIoT/tree/main/D-Link/DIR823G%20V1.0.2B05/excu_shell

Краткое описание: Отказ в обслуживании в D-Link DIR-823G firmware version 1.02B05

Идентификатор уязвимости: CVE-2023-26612

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

Уязвимый продукт: D-Link DIR-823G firmware version 1.02B05

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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: 2023-06-29 / 2023-07-06

Ссылки на источник:

- https://www.dlink.com/en/security-bulletin/
- https://github.com/726232111/VulIoT/tree/main/D-Link/DIR823G%20V1.0.2B05/HNAP1/SetParentsControlInfo

Краткое описание: Отказ в обслуживании в D-Link DIR-823G firmware version 1.02B05

Идентификатор уязвимости: CVE-2023-26616

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

Уязвимый продукт: D-Link DIR-823G firmware version 1.02B05

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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: 2023-06-29 / 2023-07-06

Ссылки на источник:

- https://www.dlink.com/en/security-bulletin/
- https://github.com/726232111/VulIoT/tree/main/D-Link/DIR823G%20V1.0.2B05/HNAP1/SetParentsControlInfo

Краткое описание: Выполнение произвольного кода в Zyxel NAS326 до V5.21, NAS540 до V5.2, NAS542 до V5.21

Идентификатор уязвимости: CVE-2023-27992

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

Уязвимый продукт: Zyxel NAS326 до V5.21, NAS540 до V5.2, NAS542 до V5.21

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

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: 2023-06-19 / 2023-06-27

Ссылки на источник:

- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-pre-authentication-command-injection-vulnerability-in-nas-products
- https://bdu.fstec.ru/vul/2023-03280

21

Краткое описание: Выполнение произвольного кода в Ubuntu

Идентификатор уязвимости: CVE-2023-37202

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Ubuntu: 20.04 - 23.04
thunderbird (Ubuntu package): до 1:102.13.0+build1-0ubuntu0.23.04.1

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

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-11 / 2023-07-11

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6214-1

22

Краткое описание: Выполнение произвольного кода в Ubuntu

Идентификатор уязвимости: CVE-2023-37201

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Ubuntu: 20.04 - 23.04
thunderbird (Ubuntu package): до 1:102.13.0+build1-0ubuntu0.23.04.1

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

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Средства устранения уязвимости: Не определено

Дата выявления / Дата обновления: 2023-07-11 / 2023-07-11

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6214-1

23

Краткое описание: Получение конфиденциальной информации в GLPI

Идентификатор уязвимости: CVE-2023-35940

Идентификатор программной ошибки: CWE-200 Разглашение важной информации лицам без соответствующих прав

Уязвимый продукт: GLPI: 9.5.0 - 10.0.7

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2023-07-10 / 2023-07-10

Ссылки на источник:

- http://github.com/glpi-project/glpi/security/advisories/GHSA-qrh8-rg45-45fw
- http://github.com/glpi-project/glpi/releases/tag/10.0.8

Краткое описание: Выполнение произвольного кода в Ubuntu

Идентификатор уязвимости: CVE-2023-34416

Идентификатор программной ошибки: CWE-119 Выполнение операций за пределами буфера памяти

Уязвимый продукт: Ubuntu: 20.04 - 23.04
thunderbird (Ubuntu package): до 1:102.13.0+build1-0ubuntu0.23.04.1

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

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.

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: 2023-07-11 / 2023-07-11

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6214-1
- https://bdu.fstec.ru/vul/2023-03125

Краткое описание: Выполнение произвольного кода в GLPI

Идентификатор уязвимости: CVE-2023-35924

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: GLPI: 10.0.0 - 10.0.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

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

Ссылки на источник:

- http://github.com/glpi-project/glpi/security/advisories/GHSA-gxh4-j63w-8jmm
- http://github.com/glpi-project/glpi/releases/tag/10.0.8

26

Краткое описание: Выполнение произвольного кода в GLPI

Идентификатор уязвимости: CVE-2023-35939

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: GLPI: 9.5.0 - 10.0.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

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: 8.1 AV:N/AC:L/PR:L/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: 2023-07-10 / 2023-07-10

Ссылки на источник:

- http://github.com/glpi-project/glpi/security/advisories/GHSA-cjcx-pwcx-v34c
- http://github.com/glpi-project/glpi/releases/tag/10.0.8

27

Краткое описание: Выполнение произвольного кода в Ubuntu

Идентификатор уязвимости: CVE-2023-36664

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

Уязвимый продукт: Ubuntu: 20.04 - 23.04
ghostscript (Ubuntu package): до 10.0.0~dfsg1-0ubuntu1.2

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

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: 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: 2023-07-10 / 2023-07-10

Ссылки на источник:

- http://ubuntu.com/security/notices/USN-6213-1
- https://bdu.fstec.ru/vul/2023-03466

Краткое описание: Выполнение произвольного кода в GLPI

Идентификатор уязвимости: CVE-2023-36808

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: GLPI: 0.80 - 10.0.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

28 **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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

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

Ссылки на источник:

- http://github.com/glpi-project/glpi/security/advisories/GHSA-vf5h-jh9q-2gjm
- http://github.com/glpi-project/glpi/releases/tag/10.0.8

Краткое описание: Выполнение произвольного кода в MOVEit Transfer

Идентификатор уязвимости: CVE-2023-36934

Идентификатор программной ошибки: CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода)

Уязвимый продукт: MOVEit Transfer: 2020.1.6 - 2020.1.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

29 **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: 9.1 AV:N/AC:L/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: 2023-07-10 / 2023-07-10

Ссылки на источник:

- http://community.progress.com/s/article/MOVEit-Transfer-2020-1-Service-Pack-July-2023
- http://www.progress.com/moveit

Краткое описание: Обход безопасности в Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions

Идентификатор уязвимости: CVE-2023-24329

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions: 8.4 - 8.4
Red Hat Enterprise Linux Server - TUS: 8.4 - 8.4
Red Hat Enterprise Linux Server - AUS: 8.4 - 8.4

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

Способ эксплуатации: Отправки специально сформированного запроса.

Последствия эксплуатации: Обход безопасности

30 **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:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Средства устранения уязвимости: Не определено

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

Ссылки на источник:

- http://access.redhat.com/errata/RHSA-2023:4004