НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2023-08-25.1 | 25 августа 2023 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-20200	Cisco FXOS	Сетевой	DoS	2023-08-25	✓
2	Высокая	CVE-2023-40481	7-Zip	Локальный	ACE	2023-08-25	✓
3	Высокая	CVE-2023-31102	7-Zip	Локальный	ACE	2023-08-25	✓
4	Высокая	CVE-2023-34359	ASUS RT-AX88U	Сетевой	DoS	2023-07-31	✓
5	Критическая	CVE-2023-35086	ASUS RT-AX56U V2 и RT-AC86U	Сетевой	ACE	2023-07-21	✓
6	Высокая	CVE-2023-37758	D-LINK DIR-815	Сетевой	DoS	2023-07-18	✗
7	Высокая	CVE-2023-34669	TOTOLINK CP300+	Сетевой	DoS	2023-07-17	✗
8	Высокая	CVE-2023-30383	TP-LINK Archer C50v2 Archer C50(US)	Сетевой	DoS	2023-07-18	✓
9	Критическая	CVE-2023-31710	TP-Link Archer AX21(US)	Сетевой	ACE	2023-08-01	✓
10	Критическая	CVE-2023-37791	D-Link DIR-619L	Сетевой	ACE	2023-07-17	✗
11	Критическая	CVE-2023-36089	D-Link DIR-645 firmware	Сетевой	PE	2023-07-31	✗
12	Критическая	CVE-2023-36090	D-Link DIR-885L	Сетевой	PE	2023-07-31	✗
13	Критическая	CVE-2023-36092	D-Link DIR-859	Сетевой	PE	2023-07-31	✗

14	Критическая	CVE-2023-36091	D-Link DIR-895	Сетевой	PE	2023-07-31	✗
15	Высокая	CVE-2023-33013	Zyxel NBG6604	Сетевой	ACE	2023-08-23	✓
16	Высокая	CVE-2023-4076	Chrome OS	Сетевой	ACE	2023-08-22	✓
17	Высокая	CVE-2023-3732	Chrome OS	Сетевой	ACE	2023-08-22	✓
18	Высокая	CVE-2023-40477	WinRAR	Локальный	ACE	2023-08-19	✓
19	Высокая	CVE-2023-4349	Google Chrome	Сетевой	ACE	2023-08-15	✓
20	Высокая	CVE-2023-4351	Google Chrome	Сетевой	ACE	2023-08-15	✓
21	Высокая	CVE-2023-4352	Google Chrome	Сетевой	ACE	2023-08-15	✓
22	Высокая	CVE-2023-4353	Google Chrome	Сетевой	ACE	2023-08-15	✓
23	Высокая	CVE-2023-4354	Google Chrome	Сетевой	ACE	2023-08-15	✓
24	Высокая	CVE-2023-4355	Google Chrome	Сетевой	ACE	2023-08-15	✓
25	Высокая	CVE-2023-4356	Google Chrome	Сетевой	OSI	2023-08-15	✓
26	Высокая	CVE-2023-4357	Google Chrome	Сетевой	OSI	2023-08-15	✓
27	Высокая	CVE-2023-2312	Google Chrome	Сетевой	ACE	2023-08-15	✓
28	Высокая	CVE-2023-4358	Google Chrome	Сетевой	OSI	2023-08-15	✓

29	Высокая	CVE-2023-4362	Google Chrome	Сетевой	ACE	2023-08-15	✓
30	Высокая	CVE-2023-4366	Google Chrome	Сетевой	OSI	2023-08-15	✓
31	Высокая	CVE-2023-4368	Google Chrome	Сетевой	OSI	2023-08-15	✓
32	Критическая	CVE-2023-40267	GitPython	Сетевой	OSI	2023-08-16	✓
33	Высокая	CVE-2023-4068	Chrome OS	Сетевой	ACE	2023-08-15	✓
34	Высокая	CVE-2023-4071	Chrome OS	Сетевой	ACE	2023-08-15	✓
35	Высокая	CVE-2023-4075	Chrome OS	Сетевой	ACE	2023-08-15	✓
36	Высокая	CVE-2023-4074	Chrome OS	Сетевой	ACE	2023-08-15	✓
37	Высокая	CVE-2023-3730	Chrome OS	Сетевой	ACE	2023-08-15	✓

1

Краткое описание: Отказ в обслуживании в Cisco FXOS

Идентификатор уязвимости: CVE-2023-20200

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Cisco FXOS: 2.0.1.37 - 2.3.1.93
UCS 6300 Series Fabric Interconnects: все версии
Firepower 4100 Series Security Appliances: все версии
Firepower 9300 Series Security Appliances: все версии
Cisco UCS: до 4.2(3d)UCSM

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fp-ucsfi-snmp-dos-qtv69NAO
- https://nvd.nist.gov/vuln/detail/CVE-2023-20200

2

Краткое описание: Выполнение произвольного кода в 7-Zip

Идентификатор уязвимости: CVE-2023-40481

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: 7-Zip: 2.00 - 22.01

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: 2023-08-25 / 2023-08-25

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1164/
- http://sourceforge.net/p/sevenzip/discussion/45797/thread/713c8a8269/
- https://bdu.fstec.ru/vul/2023-04886

3

Краткое описание: Выполнение произвольного кода в 7-Zip

Идентификатор уязвимости: CVE-2023-31102

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: 7-Zip: 2.00 - 22.01

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: 2023-08-25 / 2023-08-25

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1165/
- http://sourceforge.net/p/sevenzip/discussion/45797/thread/713c8a8269/

4

Краткое описание: Отказ в обслуживании в ASUS RT-AX88U

Идентификатор уязвимости: CVE-2023-34359

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: ASUS RT-AX88U: 3.0.0.4.388_22525-gd35b8fe

Категория уязвимого продукта: Средства защиты информации

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

Дата выявления / Дата обновления: 2023-07-31 / 2023-08-04

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-34359
- https://bdu.fstec.ru/vul/2023-04453

Краткое описание: Выполнение произвольного кода в ASUS RT-AX56U V2 и RT-AC86U

Идентификатор уязвимости: CVE-2023-35086

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

Уязвимый продукт: ASUS RT-AX56U V2 и RT-AC86U:
RT-AX56U V2: 3.0.0.4.386_50460; RT-AC86U: 3.0.0.4_386_51529

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

5 **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

Дата выявления / Дата обновления: 2023-07-21 / 2023-08-04

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-35086
- https://bdu.fstec.ru/vul/2023-04333

6

Краткое описание: Отказ в обслуживании в D-LINK DIR-815

Идентификатор уязвимости: CVE-2023-37758

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

Уязвимый продукт: D-LINK DIR-815: v1.01

Категория уязвимого продукта: Средства защиты информации

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: 2023-07-18 / 2023-07-28

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-37758

7

Краткое описание: Отказ в обслуживании в TOTOLINK CP300+

Идентификатор уязвимости: CVE-2023-34669

Идентификатор программной ошибки: Не определено

Уязвимый продукт: TOTOLINK CP300+: V5.2cu.7594

Категория уязвимого продукта: Средства защиты информации

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: 2023-07-17 / 2023-07-25

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-34669

Краткое описание: Отказ в обслуживании в TP-LINK Archer C50v2 Archer C50(US)

Идентификатор уязвимости: CVE-2023-30383

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

Уязвимый продукт: TP-LINK Archer C50v2 Archer C50(US): V2_160801
TP-LINK Archer C20v1 Archer_C20: V1_150707
TP-LINK Archer C2v1 Archer_C2_US: V1_170228

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

8 **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

Дата выявления / Дата обновления: 2023-07-18 / 2023-07-28

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-30383

Краткое описание: Выполнение произвольного кода в TP-Link Archer AX21(US)

Идентификатор уязвимости: CVE-2023-31710

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: TP-Link Archer AX21(US): V3_1.1.4 Build 20230219 и V3.6_1.1.4 Build 20230219

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

9 **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

Дата выявления / Дата обновления: 2023-08-01 / 2023-08-04

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-31710

10

Краткое описание: Выполнение произвольного кода в D-Link DIR-619L

Идентификатор уязвимости: CVE-2023-37791

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: D-Link DIR-619L: 2.04 (TW)

Категория уязвимого продукта: Средства защиты информации

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: 2023-07-17 / 2023-07-27

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-37791
- https://bdu.fstec.ru/vul/2023-04594

Краткое описание: Повышение привилегий в D-Link DIR-645 firmware

Идентификатор уязвимости: CVE-2023-36089

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: D-Link DIR-645 firmware: 1.03

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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: 2023-07-31 / 2023-08-04

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-36089

Краткое описание: Повышение привилегий в D-Link DIR-885L

Идентификатор уязвимости: CVE-2023-36090

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: D-Link DIR-885L: FW102b01

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

12 **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: 2023-07-31 / 2023-08-04

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-36090

13

Краткое описание: Повышение привилегий в D-Link DIR-859

Идентификатор уязвимости: CVE-2023-36092

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: D-Link DIR-859: FW105b03

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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: 2023-07-31 / 2023-08-04

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-36092
- https://bdu.fstec.ru/vul/2023-04335

14

Краткое описание: Повышение привилегий в D-Link DIR-895

Идентификатор уязвимости: CVE-2023-36091

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: D-Link DIR-895: FW102b07

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

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: 2023-07-31 / 2023-08-04

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2023-36091
- https://bdu.fstec.ru/vul/2023-04359

15

Краткое описание: Выполнение произвольного кода в Zyxel NBG6604

Идентификатор уязвимости: CVE-2023-33013

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

Уязвимый продукт: Zyxel NBG6604: 1.01(ABIR.1)C0

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: 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

Дата выявления / Дата обновления: 2023-08-23 / 2023-08-23

Ссылки на источник:

- http://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-in-ntp-feature-of-nbg6604-home-router
- https://bdu.fstec.ru/vul/2023-04707

16

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-4076

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 108.0.5359.240

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

Дата выявления / Дата обновления: 2023-08-22 / 2023-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/long-term-support-channel-update-for_21.html
- https://bdu.fstec.ru/vul/2023-04492

17

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-3732

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

Уязвимый продукт: Chrome OS: до 108.0.5359.240

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

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: 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

Дата выявления / Дата обновления: 2023-08-22 / 2023-08-22

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/long-term-support-channel-update-for_21.html
- https://bdu.fstec.ru/vul/2023-04003

18

Краткое описание: Выполнение произвольного кода в WinRAR

Идентификатор уязвимости: CVE-2023-40477

Идентификатор программной ошибки: CWE-129 Некорректная проверка индекса массива

Уязвимый продукт: WinRAR: 6.00 - 6.22 beta 1

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: 2023-08-19 / 2023-08-19

Ссылки на источник:

- http://www.zerodayinitiative.com/advisories/ZDI-23-1152/
- http://www.win-rar.com/singlenewsview.html?&L=0&tx_ttnews%5Btt_news%5D=232&cHash=c5bf79590657e32554c6683296a8e8aa

19

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-4349

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

Категория уязвимого продукта: Прикладное программное обеспечение

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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1458303
- https://bdu.fstec.ru/vul/2023-04873

20

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-4351

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

Категория уязвимого продукта: Прикладное программное обеспечение

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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1465833
- https://bdu.fstec.ru/vul/2023-04851

21

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-4352

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

Категория уязвимого продукта: Прикладное программное обеспечение

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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1452076
- https://bdu.fstec.ru/vul/2023-04870

22

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-4353

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

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: 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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1458046
- https://bdu.fstec.ru/vul/2023-04869

23

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-4354

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

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: 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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1464215
- https://bdu.fstec.ru/vul/2023-04861

24

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-4355

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1468943
- https://bdu.fstec.ru/vul/2023-04871

25

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4356

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1449929
- https://bdu.fstec.ru/vul/2023-04855

26

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4357

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1458911
- https://bdu.fstec.ru/vul/2023-04875

27

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-2312

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

Категория уязвимого продукта: Прикладное программное обеспечение

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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1448548
- https://bdu.fstec.ru/vul/2023-04872

28

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4358

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1466415
- https://bdu.fstec.ru/vul/2023-04856

29

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2023-4362

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

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: 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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1316379
- https://bdu.fstec.ru/vul/2023-04876

30

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4366

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1450784
- https://bdu.fstec.ru/vul/2023-04859

31

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2023-4368

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 115.0.5790.171

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/stable-channel-update-for-desktop_15.html
- http://crbug.com/1467751
- https://bdu.fstec.ru/vul/2023-04847

32

Краткое описание: Получение конфиденциальной информации в GitPython

Идентификатор уязвимости: CVE-2023-40267

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: GitPython: 3.1.0 - 3.1.31

Категория уязвимого продукта: Прикладное программное обеспечение

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.

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: 2023-08-16 / 2023-08-16

Ссылки на источник:

- http://github.com/gitpython-developers/GitPython/commit/ca965ecc81853bca7675261729143f54e5bf4cdd
- http://github.com/gitpython-developers/GitPython/pull/1609

33

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-4068

Идентификатор программной ошибки: CWE-843 Доступ к ресурсам с использованием несовместимых типов (смешение типов)

Уязвимый продукт: Chrome OS: до 114.0.5735.329

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/long-term-support-channel-update-for_14.html
- https://bdu.fstec.ru/vul/2023-04416

34

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-4071

Идентификатор программной ошибки: CWE-122 Переполнение буфера в динамической памяти

Уязвимый продукт: Chrome OS: до 114.0.5735.329

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/long-term-support-channel-update-for_14.html
- https://bdu.fstec.ru/vul/2023-04489

35

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-4075

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 114.0.5735.329

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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/long-term-support-channel-update-for_14.html
- https://bdu.fstec.ru/vul/2023-04493

36

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-4074

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 114.0.5735.329

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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/long-term-support-channel-update-for_14.html
- https://bdu.fstec.ru/vul/2023-04494

37

Краткое описание: Выполнение произвольного кода в Chrome OS

Идентификатор уязвимости: CVE-2023-3730

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 114.0.5735.329

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

Дата выявления / Дата обновления: 2023-08-15 / 2023-08-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2023/08/long-term-support-channel-update-for_14.html
- https://bdu.fstec.ru/vul/2023-04001