НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-05-13.1 | 13 мая 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2023-50009	FFmpeg	Локальный	ACE	2024-05-09	✓
2	Высокая	CVE-2023-50010	FFmpeg	Сетевой	ACE	2024-05-09	✓
3	Критическая	CVE-2023-50007	FFmpeg	Сетевой	ACE	2024-05-09	✓
4	Критическая	CVE-2023-51798	FFmpeg	Сетевой	ACE	2024-05-09	✓
5	Критическая	CVE-2023-51797	FFmpeg	Сетевой	ACE	2024-05-09	✓
6	Критическая	CVE-2023-51796	FFmpeg	Сетевой	ACE	2024-05-09	✓
7	Критическая	CVE-2023-51795	FFmpeg	Сетевой	ACE	2024-05-09	✓
8	Высокая	CVE-2023-51793	FFmpeg	Сетевой	ACE	2024-05-09	✓
9	Критическая	CVE-2023-50008	FFmpeg	Сетевой	ACE	2024-05-09	✓
10	Критическая	CVE-2023-51791	FFmpeg	Сетевой	ACE	2024-05-09	✓
11	Высокая	CVE-2023-49501	FFmpeg	Локальный	ACE	2024-05-09	✓
12	Критическая	CVE-2024-32739	CyberPower PowerPanel Enterprise	Сетевой	ACE	2024-05-10	✓
13	Критическая	CVE-2024-32738	CyberPower PowerPanel Enterprise	Сетевой	ACE	2024-05-10	✓

14	Критическая	CVE-2024-32737	CyberPower PowerPanel Enterprise	Сетевой	ACE	2024-05-10	✓
15	Высокая	CVE-2024-31582	FFmpeg	Сетевой	ACE	2024-05-09	✓
16	Критическая	CVE-2024-32736	CyberPower PowerPanel Enterprise	Сетевой	ACE	2024-05-10	✓
17	Критическая	CVE-2024-31581	FFmpeg	Сетевой	ACE	2024-05-09	✓
18	Критическая	CVE-2024-32735	CyberPower PowerPanel Enterprise	Сетевой	SB	2024-05-10	✓
19	Критическая	CVE-2024-27793	Apple iTunes	Сетевой	ACE	2024-05-08	✓
20	Критическая	CVE-2023-49528	FFmpeg	Сетевой	ACE	2024-05-09	✓
21	Высокая	CVE-2023-49502	FFmpeg	Сетевой	ACE	2024-05-09	✓
22	Высокая	CVE-2023-43887	libde265	Сетевой	ACE	2024-05-09	✓
23	Высокая	CVE-2023-27103	libde265	Сетевой	ACE	2024-05-09	✓
24	Высокая	CVE-2024-4549	Delta Electronics DIAEnergie	Сетевой	DoS	2024-05-07	✓
25	Критическая	CVE-2024-4548	Delta Electronics DIAEnergie	Сетевой	ACE	2024-05-07	✓
26	Критическая	CVE-2024-34402	uriparser	Сетевой	ACE	2024-05-06	✓
27	Критическая	CVE-2024-4547	Delta Electronics DIAEnergie	Сетевой	ACE	2024-05-07	✓
28	Критическая	CVE-2024-34403	uriparser	Сетевой	ACE	2024-05-06	✓

29	Критическая	CVE-2023-37895	Cloudera Data Platform Private Cloud Base with IBM (CDP)	Сетевой	ACE	2024-05-10	✓
30	Критическая	CVE-2023-34478	Cloudera Data Platform Private Cloud Base with IBM (CDP)	Сетевой	SB	2024-05-10	✓
31	Критическая	CVE-2023-25613	Cloudera Data Platform Private Cloud Base with IBM (CDP)	Сетевой	SB	2024-05-10	✓
32	Критическая	CVE-2024-33722	SOPlanning	Сетевой	ACE	2024-05-10	✓
33	Высокая	CVE-2024-30055	Microsoft Edge	Сетевой	XSS\CSS	2024-05-12	✓
34	Высокая	CVE-2024-31856	CyberPower PowerPanel	Сетевой	ACE	2024-05-03	✓
35	Критическая	CVE-2024-32047	CyberPower PowerPanel	Сетевой	OSI	2024-05-03	✓
36	Критическая	CVE-2024-32053	CyberPower PowerPanel	Сетевой	ACE	2024-05-03	✓
37	Высокая	CVE-2024-33615	CyberPower PowerPanel	Сетевой	ACE	2024-05-03	✓
38	Критическая	CVE-2024-34025	CyberPower PowerPanel	Сетевой	PE	2024-05-03	✓
39	Высокая	CVE-2024-4622	Alpitronic Hypercharger EV Charger	Сетевой	OSI	2024-05-10	✗
40	Высокая	CVE-2024-23473	SolarWinds Access Rights Manager	Сетевой	ACE	2024-05-10	✓
41	Высокая	CVE-2023-49465	libde265	Сетевой	ACE	2024-05-09	✓
42	Высокая	CVE-2023-49467	libde265	Сетевой	ACE	2024-05-09	✓

43	Высокая	CVE-2024-28075	SolarWinds Access Rights Manager	Сетевой	ACE	2024-05-10	✓
44	Высокая	CVE-2023-49468	libde265	Сетевой	ACE	2024-05-09	✓
45	Высокая	CVE-2024-3298	Dassault Systmes eDrawings	Локальный	ACE	2024-05-10	✓
46	Высокая	CVE-2024-4671	Google Chrome	Сетевой	ACE	2024-05-10	✓
47	Высокая	CVE-2024-25710	TPF Toolkit	Локальный	DoS	2024-05-09	✓
48	Высокая	CVE-2024-21793	F5 BIG-IP Next Central Manager API	Сетевой	WLF	2024-05-09	✓
49	Высокая	CVE-2024-26026	F5 BIG-IP Next Central Manager API	Сетевой	RLF	2024-05-09	✓
50	Высокая	CVE-2024-4559	Google Chrome	Сетевой	ACE	2024-05-07	✓
51	Высокая	CVE-2024-4558	Google Chrome	Сетевой	ACE	2024-05-07	✓
52	Высокая	CVE-2023-45681	stb_vorbis.c	Локальный	ACE	2024-05-06	✗
53	Критическая	CVE-2023-47212	stb_vorbis.c	Сетевой	ACE	2024-05-06	✗
54	Высокая	CVE-2024-32866	Conform	Сетевой	ACE	2024-05-06	✓
55	Высокая	CVE-2024-2410	Protobuf	Сетевой	ACE	2024-05-06	✓
56	Высокая	CVE-2024-20353	Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services	Сетевой	DoS	2024-04-24	✓

57	Высокая	CVE-2024-20313	Cisco IOS XE Software	Смежная сеть	DoS	2024-03-28	✓
58	Высокая	CVE-2024-3385	Palo Alto PAN-OS	Сетевой	DoS	2024-04-12	✓
59	Высокая	CVE-2024-3384	Palo Alto PAN-OS	Сетевой	DoS	2024-04-12	✓
60	Высокая	CVE-2024-4368	Microsoft Edge	Сетевой	ACE	2024-05-03	✓
61	Высокая	CVE-2024-4331	Microsoft Edge	Сетевой	ACE	2024-05-03	✓
62	Критическая	CVE-2023-49606	Tinyproxy	Сетевой	ACE	2024-05-02	✗

1

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-50009

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Дата выявления / Дата обновления: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10699

2

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-50010

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Дата выявления / Дата обновления: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10702

3

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-50007

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://github.com/FFmpeg/FFmpeg/commit/b1942734c7cbcdc9034034373abcc9ecb9644c47
- http://trac.ffmpeg.org/ticket/10700

4

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-51798

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10758

5

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-51797

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10756

6

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-51796

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10753

7

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-51795

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10749

8

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-51793

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Дата выявления / Дата обновления: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10743

9

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-50008

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://github.com/FFmpeg/FFmpeg/commit/5f87a68cf70dafeab2fb89b42e41a4c29053b89b
- http://trac.ffmpeg.org/ticket/10701

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-51791

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

10 **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: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10738

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-49501

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10686

Краткое описание: Выполнение произвольного кода в CyberPower PowerPanel Enterprise

Идентификатор уязвимости: CVE-2024-32739

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

Уязвимый продукт: PowerPanel Enterprise: до 2.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-14

Краткое описание: Выполнение произвольного кода в CyberPower PowerPanel Enterprise

Идентификатор уязвимости: CVE-2024-32738

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

Уязвимый продукт: PowerPanel Enterprise: до 2.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-14

Краткое описание: Выполнение произвольного кода в CyberPower PowerPanel Enterprise

Идентификатор уязвимости: CVE-2024-32737

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

Уязвимый продукт: PowerPanel Enterprise: до 2.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

14

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: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-14

15

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2024-31582

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 7.5 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: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://github.com/FFmpeg/FFmpeg/blob/n6.1.1/libavfilter/vf_codecview.c#L220
- http://github.com/ffmpeg/ffmpeg/commit/99debe5f823f45a482e1dc08de35879aa9c74bd2
- http://gist.github.com/1047524396/b47d5efe3bc420fb91dbb77c73c0fff3

Краткое описание: Выполнение произвольного кода в CyberPower PowerPanel Enterprise

Идентификатор уязвимости: CVE-2024-32736

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

Уязвимый продукт: PowerPanel Enterprise: до 2.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

16

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: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-14

17

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2024-31581

Идентификатор программной ошибки: CWE-129 Некорректная проверка индекса массива

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://github.com/ffmpeg/ffmpeg/commit/ce0c178a408d43e71085c28a47d50dc939b60196
- http://github.com/FFmpeg/FFmpeg/blob/n6.1.1/libavcodec/cbs_h266_syntax_template.c#L2048
- http://gist.github.com/1047524396/a7e9273e1255377582678403533 3cdd8

18

Краткое описание: Обход безопасности в CyberPower PowerPanel Enterprise

Идентификатор уязвимости: CVE-2024-32735

Идентификатор программной ошибки: CWE-306 Отсутствие аутентификации для критически важных функций

Уязвимый продукт: PowerPanel Enterprise: до 2.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-14

19

Краткое описание: Выполнение произвольного кода в Apple iTunes

Идентификатор уязвимости: CVE-2024-27793

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

Уязвимый продукт: iTunes: 12.0 - 12.13.1.3

Категория уязвимого продукта: Операционные системы Apple 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: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-08 / 2024-05-08

Ссылки на источник:

- http://support.apple.com/en-us/HT214099

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-49528

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

20 **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: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10691

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2023-49502

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

Уязвимый продукт: FFmpeg: все версии

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

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: 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: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://trac.ffmpeg.org/ticket/10688

Краткое описание: Выполнение произвольного кода в libde265

Идентификатор уязвимости: CVE-2023-43887

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

Уязвимый продукт: libde265: 1.0.0 - 1.0.12

Категория уязвимого продукта: Не определено

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.

22

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://github.com/strukturag/libde265/issues/418
- http://github.com/strukturag/libde265/commit/63b596c915977f038eafd7647d1db25488a8c133
- http://lists.debian.org/debian-lts-announce/2023/11/msg00032.html
- https://bdu.fstec.ru/vul/2024-02536

23

Краткое описание: Выполнение произвольного кода в libde265

Идентификатор уязвимости: CVE-2023-27103

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

Уязвимый продукт: libde265: 1.0.0 - 1.0.11

Категория уязвимого продукта: Не определено

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

Дата выявления / Дата обновления: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://github.com/strukturag/libde265/issues/394
- http://lists.debian.org/debian-lts-announce/2023/11/msg00032.html
- https://bdu.fstec.ru/vul/2023-02130

Краткое описание: Отказ в обслуживании в Delta Electronics DIAEnergie

Идентификатор уязвимости: CVE-2024-4549

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: DIAEnergie: 1.10.1.8610

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

24 **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: 2024-05-07 / 2024-05-07

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-13

Краткое описание: Выполнение произвольного кода в Delta Electronics DIAEnergie

Идентификатор уязвимости: CVE-2024-4548

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

Уязвимый продукт: DIAEnergie: 1.10.1.8610

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

25

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: 2024-05-07 / 2024-05-07

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-13

26

Краткое описание: Выполнение произвольного кода в uriparser

Идентификатор уязвимости: CVE-2024-34402

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: uriparser: 0.3 - 0.9.7

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-06 / 2024-05-06

Ссылки на источник:

- http://github.com/uriparser/uriparser/pull/185
- http://github.com/uriparser/uriparser/issues/183

Краткое описание: Выполнение произвольного кода в Delta Electronics DIAEnergie

Идентификатор уязвимости: CVE-2024-4547

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

Уязвимый продукт: DIAEnergie: 1.10.1.8610

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

27

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: 2024-05-07 / 2024-05-07

Ссылки на источник:

- http://www.tenable.com/security/research/tra-2024-13

28

Краткое описание: Выполнение произвольного кода в uriparser

Идентификатор уязвимости: CVE-2024-34403

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: uriparser: 0.3 - 0.9.7

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-06 / 2024-05-06

Ссылки на источник:

- http://github.com/uriparser/uriparser/issues/183
- http://github.com/uriparser/uriparser/pull/186

29

Краткое описание: Выполнение произвольного кода в Cloudera Data Platform Private Cloud Base with IBM (CDP)

Идентификатор уязвимости: CVE-2023-37895

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Cloudera Data Platform Private Cloud Base for IBM: до 7.1.9.3 HF2

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://www.ibm.com/support/pages/node/7150430
- https://bdu.fstec.ru/vul/2023-06209

30

Краткое описание: Обход безопасности в Cloudera Data Platform Private Cloud Base with IBM (CDP)

Идентификатор уязвимости: CVE-2023-34478

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: Cloudera Data Platform Private Cloud Base for IBM: до 7.1.9.3 HF2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Обход безопасности

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: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://www.ibm.com/support/pages/node/7150430
- https://bdu.fstec.ru/vul/2023-04307

Краткое описание: Обход безопасности в Cloudera Data Platform Private Cloud Base with IBM (CDP)

Идентификатор уязвимости: CVE-2023-25613

Идентификатор программной ошибки: CWE-90 Некорректная нейтрализация специальных элементов, используемых в LDAP-запросах (внедрение LDAP)

Уязвимый продукт: Cloudera Data Platform Private Cloud Base for IBM: до 7.1.9.3 HF2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Обход безопасности

31

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: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://www.ibm.com/support/pages/node/7150430

Краткое описание: Выполнение произвольного кода в SOPlanning

Идентификатор уязвимости: CVE-2024-33722

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

Уязвимый продукт: SOPlanning: 1.52

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

32

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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://github.com/fuzzlove/soplanning-1.52-exploits

Краткое описание: Межсайтовый скриптинг в Microsoft Edge

Идентификатор уязвимости: CVE-2024-30055

Идентификатор программной ошибки: CWE-451 Некорректное представление важной информации интерфейсом пользователя

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 124.0.2478.80

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: Межсайтовый скриптинг

33 **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

Дата выявления / Дата обновления: 2024-05-12 / 2024-05-12

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-30055

Краткое описание: Выполнение произвольного кода в CyberPower PowerPanel

Идентификатор уязвимости: CVE-2024-31856

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

Уязвимый продукт: PowerPanel: 4.9.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

34 **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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-03 / 2024-05-03

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-123-01
- https://bdu.fstec.ru/vul/2024-03467

35

Краткое описание: Получение конфиденциальной информации в CyberPower PowerPanel

Идентификатор уязвимости: CVE-2024-32047

Идентификатор программной ошибки: CWE-489 Присутствует код отладки

Уязвимый продукт: PowerPanel: 4.9.0

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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-03 / 2024-05-03

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-123-01
- https://bdu.fstec.ru/vul/2024-03464

36

Краткое описание: Выполнение произвольного кода в CyberPower PowerPanel

Идентификатор уязвимости: CVE-2024-32053

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: PowerPanel: 4.9.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование жестко закодированных учетных 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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-03 / 2024-05-03

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-123-01
- https://bdu.fstec.ru/vul/2024-03469

37

Краткое описание: Выполнение произвольного кода в CyberPower PowerPanel

Идентификатор уязвимости: CVE-2024-33615

Идентификатор программной ошибки: CWE-22 Некорректные ограничения путей для каталогов (выход за пределы каталога)

Уязвимый продукт: PowerPanel: 4.9.0

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: 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-03 / 2024-05-03

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-123-01
- https://bdu.fstec.ru/vul/2024-03470

38

Краткое описание: Повышение привилегий в CyberPower PowerPanel

Идентификатор уязвимости: CVE-2024-34025

Идентификатор программной ошибки: CWE-259 Использование жестко закодированного пароля

Уязвимый продукт: PowerPanel: 4.9.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-03 / 2024-05-03

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-123-01
- https://bdu.fstec.ru/vul/2024-03471

Краткое описание: Получение конфиденциальной информации в Alpitronic Hypercharger EV Charger

Идентификатор уязвимости: CVE-2024-4622

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Hypercharger EV charger: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Получение конфиденциальной информации

39

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

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-130-02

40

Краткое описание: Выполнение произвольного кода в SolarWinds Access Rights Manager

Идентификатор уязвимости: CVE-2024-23473

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: Access Rights Manager: 2023.2 - 2023.2.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Использование жестко закодированных учетных 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

Дата выявления / Дата обновления: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://documentation.solarwinds.com/en/Success_Center/ARM/Content/release_notes/arm_2023-2-4_release_notes.htm

41

Краткое описание: Выполнение произвольного кода в libde265

Идентификатор уязвимости: CVE-2023-49465

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

Уязвимый продукт: libde265: 1.0.0 - 1.0.14

Категория уязвимого продукта: Не определено

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

Дата выявления / Дата обновления: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://github.com/strukturag/libde265/issues/435
- http://lists.debian.org/debian-lts-announce/2023/12/msg00022.html
- https://bdu.fstec.ru/vul/2024-00520

42

Краткое описание: Выполнение произвольного кода в libde265

Идентификатор уязвимости: CVE-2023-49467

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

Уязвимый продукт: libde265: 1.0.0 - 1.0.14

Категория уязвимого продукта: Не определено

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

Дата выявления / Дата обновления: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://github.com/strukturag/libde265/issues/434
- http://lists.debian.org/debian-lts-announce/2023/12/msg00022.html
- https://bdu.fstec.ru/vul/2024-01356

Краткое описание: Выполнение произвольного кода в SolarWinds Access Rights Manager

Идентификатор уязвимости: CVE-2024-28075

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Access Rights Manager: 2023.2 - 2023.2.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

43 **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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://documentation.solarwinds.com/en/Success_Center/ARM/Content/release_notes/arm_2023-2-4_release_notes.htm

Краткое описание: Выполнение произвольного кода в libde265

Идентификатор уязвимости: CVE-2023-49468

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: libde265: 1.0.0 - 1.0.14

Категория уязвимого продукта: Не определено

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.

44

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: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://github.com/strukturag/libde265/issues/432
- http://lists.debian.org/debian-lts-announce/2023/12/msg00022.html
- https://bdu.fstec.ru/vul/2024-01357

Краткое описание: Выполнение произвольного кода в Dassault Systmes eDrawings

Идентификатор уязвимости: CVE-2024-3298

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: eDrawings: SOLIDWORKS 2023 - SOLIDWORKS 2024

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.

45

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: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://www.3ds.com/vulnerability/advisories
- http://www.zerodayinitiative.com/advisories/ZDI-24-438/
- http://www.zerodayinitiative.com/advisories/ZDI-24-437/
- http://www.zerodayinitiative.com/advisories/ZDI-24-436/
- http://www.zerodayinitiative.com/advisories/ZDI-24-435/
- http://www.zerodayinitiative.com/advisories/ZDI-24-433/
- http://www.zerodayinitiative.com/advisories/ZDI-24-431/
- http://www.zerodayinitiative.com/advisories/ZDI-24-429/

46

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-4671

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 124.0.6367.156

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: 2024-05-10 / 2024-05-10

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_9.html
- http://crbug.com/339266700

47

Краткое описание: Отказ в обслуживании в TPF Toolkit

Идентификатор уязвимости: CVE-2024-25710

Идентификатор программной ошибки: CWE-835 Бесконечный цикл (зацикливание)

Уязвимый продукт: TPF Toolkit: до 4.6 FP18

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://www.ibm.com/support/pages/node/7150637
- https://bdu.fstec.ru/vul/2024-02851

Краткое описание: Запись локальных файлов в F5 BIG-IP Next Central Manager API

Идентификатор уязвимости: CVE-2024-21793

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

Уязвимый продукт: BIG-IP Next Central Manager: с версии 20.0.1 по 20.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Запись локальных файлов

48

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

Дата выявления / Дата обновления: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://my.f5.com/manage/s/article/K000138733

Краткое описание: Чтение локальных файлов в F5 BIG-IP Next Central Manager API

Идентификатор уязвимости: CVE-2024-26026

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

Уязвимый продукт: BIG-IP Next Central Manager: с версии 20.0.1 по 20.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Чтение локальных файлов

49

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

Дата выявления / Дата обновления: 2024-05-09 / 2024-05-09

Ссылки на источник:

- http://my.f5.com/manage/s/article/K000138733

50

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-4559

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 124.0.6367.119

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: 2024-05-07 / 2024-05-07

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_7.html
- http://crbug.com/331369797

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-4558

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 124.0.6367.119

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

51

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: 2024-05-07 / 2024-05-07

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/05/stable-channel-update-for-desktop_7.html
- http://crbug.com/337766133

Краткое описание: Выполнение произвольного кода в stb_vorbis.c

Идентификатор уязвимости: CVE-2023-45681

Идентификатор программной ошибки: CWE-190 Целочисленное переполнение или циклический возврат

Уязвимый продукт: stb_vorbis.c: версии 1.22

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2024-05-06 / 2024-05-06

Ссылки на источник:

- http://github.com/nothings/stb/blob/5736b15f7ea0ffb08dd38af21067c314d6a3aae9/stb_vorbis.c#L3660-L3677
- http://securitylab.github.com/advisories/GHSL-2023-145_GHSL-2023-151_stb_image_h/

Краткое описание: Выполнение произвольного кода в stb_vorbis.c

Идентификатор уязвимости: CVE-2023-47212

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

Уязвимый продукт: stb_vorbis.c: версии 1.22

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

53 **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: 2024-05-06 / 2024-05-06

Ссылки на источник:

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1846

54

Краткое описание: Выполнение произвольного кода в Conform

Идентификатор уязвимости: CVE-2024-32866

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Conform: с версии 0.0.1 по 1.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-05-06 / 2024-05-06

Ссылки на источник:

- http://github.com/edmundhung/conform/security/advisories/GHSA-624g-8qjg-8qxf
- http://github.com/edmundhung/conform/commit/4819d51b5a53fd5486fc85c17cdc148eb160e3de
- http://github.com/edmundhung/conform/blob/59156d7115a7207fa3b6f8a70a4342a9b24c2501/packages/conform-dom/formdata.ts#L117

Краткое описание: Выполнение произвольного кода в Protobuf

Идентификатор уязвимости: CVE-2024-2410

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: protobuf: 4.22.0 - 4.24.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

55 **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

Дата выявления / Дата обновления: 2024-05-06 / 2024-05-06

Ссылки на источник:

- http://github.com/protocolbuffers/protobuf/releases/tag/v25.0

56

Краткое описание: Отказ в обслуживании в Cisco Adaptive Security Appliance and Firepower Threat Defense Software Web Services

Идентификатор уязвимости: CVE-2024-20353

Идентификатор программной ошибки: CWE-835 Бесконечный цикл (зацикливание)

Уязвимый продукт: Cisco Adaptive Security Appliance (ASA): до 9.20.2.10
Cisco Firepower Threat Defense (FTD): до 9.20.2.10

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-04-24 / 2024-04-24

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-websrvs-dos-X8gNucD2
- http://bst.cloudapps.cisco.com/bugsearch/bug/CSCwj10955
- http://blog.talosintelligence.com/arcanedoor-new-espionage-focused-campaign-found-targeting-perimeter-network-devices/
- https://bdu.fstec.ru/vul/2024-03233

Краткое описание: Отказ в обслуживании в Cisco IOS XE Software

Идентификатор уязвимости: CVE-2024-20313

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

Уязвимый продукт: Cisco IOS XE: с версии 17.6.5 по 17.12.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

57 **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:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-03-28 / 2024-03-28

Ссылки на источник:

- http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ospf-dos-dR9Sfrxp

58

Краткое описание: Отказ в обслуживании в Palo Alto PAN-OS

Идентификатор уязвимости: CVE-2024-3385

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Palo Alto PAN-OS: с версии 9.0 по 11.0.2-h3

Категория уязвимого продукта: Unix-подобные операционные системы 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

Дата выявления / Дата обновления: 2024-04-12 / 2024-04-12

Ссылки на источник:

- http://security.paloaltonetworks.com/CVE-2024-3385
- https://bdu.fstec.ru/vul/2024-03099

59

Краткое описание: Отказ в обслуживании в Palo Alto PAN-OS

Идентификатор уязвимости: CVE-2024-3384

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Palo Alto PAN-OS: с версии 8.1 по 10.0.12-h1

Категория уязвимого продукта: Unix-подобные операционные системы 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

Дата выявления / Дата обновления: 2024-04-12 / 2024-04-12

Ссылки на источник:

- http://security.paloaltonetworks.com/CVE-2024-3384
- https://bdu.fstec.ru/vul/2024-03069

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-4368

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 124.0.2478.67

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

60

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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-03 / 2024-05-03

Ссылки на источник:

- http://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-4368

61

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-4331

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 124.0.2478.67

Категория уязвимого продукта: Операционные системы Microsoft 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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-05-03 / 2024-05-03

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-4331

Краткое описание: Выполнение произвольного кода в Tinyproxy

Идентификатор уязвимости: CVE-2023-49606

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: tinyproxy: 1.10.0 - 1.11.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Выполнение произвольного кода

62

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: 2024-05-02 / 2024-05-02

Ссылки на источник:

- http://talosintelligence.com/vulnerability_reports/TALOS-2023-1889