НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2024-07-01.1 | 1 июля 2024 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-33883	ejs	Сетевой	ACE	2024-06-28	✓
2	Критическая	CVE-2024-6071	PTC Creo Elements/Direct License Server	Сетевой	ACE	2024-06-28	✓
3	Критическая	CVE-2024-5276	Fortra FileCatalyst Workflow	Сетевой	ACE	2024-06-28	✓
4	Критическая	CVE-2024-5805	MOVEit Gateway	Сетевой	SB	2024-06-28	✓
5	Высокая	CVE-2024-34122	Microsoft Edge	Сетевой	ACE	2024-06-27	✓
6	Критическая	CVE-2024-5806	MOVEit Transfer	Сетевой	SB	2024-06-26	✓
7	Высокая	CVE-2023-4727	Dogtag PKI	Смежная сеть	SB	2024-06-25	✓
8	Высокая	CVE-2024-6293	Google Chrome	Сетевой	ACE	2024-06-25	✓
9	Высокая	CVE-2024-6292	Google Chrome	Сетевой	ACE	2024-06-25	✓
10	Высокая	CVE-2024-6291	Google Chrome	Сетевой	ACE	2024-06-25	✓
11	Высокая	CVE-2024-6290	Google Chrome	Сетевой	ACE	2024-06-25	✓
12	Критическая	CVE-2024-29868	Apache StreamPipes	Сетевой	OSI	2024-06-24	✓
13	Высокая	CVE-2024-39331	Emacs	Сетевой	ACE	2024-06-24	✓

1

Краткое описание: Выполнение произвольного кода в ejs

Идентификатор уязвимости: CVE-2024-33883

Идентификатор программной ошибки: Не определено

Уязвимый продукт: ejs: 2.0.1 - 3.1.9

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/E:P/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-28 / 2024-06-28

Ссылки на источник:

- http://github.com/mde/ejs/commit/e469741dca7df2eb400199e1cdb74621e3f89aa5
- http://github.com/mde/ejs/compare/v3.1.9...v3.1.10
- http://security.netapp.com/advisory/ntap-20240605-0003/

2

Краткое описание: Выполнение произвольного кода в PTC Creo Elements/Direct License Server

Идентификатор уязвимости: CVE-2024-6071

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

Уязвимый продукт: Creo Elements/Direct License Server: 20.7.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-28 / 2024-06-28

Ссылки на источник:

- http://www.cisa.gov/news-events/ics-advisories/icsa-24-177-02
- http://www.ptc.com/en/support/article/CS417607

3

Краткое описание: Выполнение произвольного кода в Fortra FileCatalyst Workflow

Идентификатор уязвимости: CVE-2024-5276

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

Уязвимый продукт: FileCatalyst Workflow: до 5.1.6 139

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2024-06-28 / 2024-06-28

Ссылки на источник:

- http://www.fortra.com/security/advisory/fi-2024-008
- http://www.tenable.com/security/research/tra-2024-25
- https://bdu.fstec.ru/vul/2024-04812

4

Краткое описание: Обход безопасности в MOVEit Gateway

Идентификатор уязвимости: CVE-2024-5805

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: MOVEit Gateway: 2024.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 9.1 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: 2024-06-28 / 2024-06-28

Ссылки на источник:

- http://community.progress.com/s/article/MOVEit-Gateway-Critical-Security-Alert-Bulletin-June-2024-CVE-2024-5805

5

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2024-34122

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Microsoft Edge: 79.0.309.71 - 126.0.2592.68

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла в браузере.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-27 / 2024-06-27

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2024-34122

6

Краткое описание: Обход безопасности в MOVEit Transfer

Идентификатор уязвимости: CVE-2024-5806

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: MOVEit Transfer: 2023.0 - 2024.0.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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: 9.1 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: 2024-06-26 / 2024-06-26

Ссылки на источник:

- http://community.progress.com/s/article/MOVEit-Transfer-Product-Security-Alert-Bulletin-June-2024-CVE-2024-5806
- http://x.com/Shadowserver/status/1805676078620401831
- https://bdu.fstec.ru/vul/2024-04809

7

Краткое описание: Обход безопасности в Dogtag PKI

Идентификатор уязвимости: CVE-2023-4727

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

Уязвимый продукт: PKI: 11.0.0 - 11.4.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Некорректная проверка входных данных.

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-25 / 2024-06-25

Ссылки на источник:

- http://bugzilla.redhat.com/show_bug.cgi?id=2232218
- http://github.com/dogtagpki/pki/commit/54e5b3c5932ad634b5ddf5b1d4d88c9419d6f720
- http://github.com/dogtagpki/pki/commit/aa7161ba378caf5cf0471aafb679a842679c8388

8

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6293

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 126.0.6478.116

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-25 / 2024-06-25

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop_24.html
- http://crbug.com/345993680

9

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6292

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 126.0.6478.116

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-25 / 2024-06-25

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop_24.html
- http://crbug.com/342545100

10

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6291

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 126.0.6478.116

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-25 / 2024-06-25

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop_24.html
- http://crbug.com/40942995

11

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6290

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 126.0.6478.116

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-06-25 / 2024-06-25

Ссылки на источник:

- http://chromereleases.googleblog.com/2024/06/stable-channel-update-for-desktop_24.html
- http://crbug.com/342428008

Краткое описание: Получение конфиденциальной информации в Apache StreamPipes

Идентификатор уязвимости: CVE-2024-29868

Идентификатор программной ошибки: CWE-338 Использование ненадежного ГПСЧ

Уязвимый продукт: StreamPipes: 0.69.0 - 0.93.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-06-24 / 2024-06-24

Ссылки на источник:

- http://lists.apache.org/thread/zqn5z48gz7bp0q8ctk96ht8bc7vd3njv

Краткое описание: Выполнение произвольного кода в Emacs

Идентификатор уязвимости: CVE-2024-39331

Идентификатор программной ошибки: CWE-676 Использование потенциально опасной функции

Уязвимый продукт: Emacs: 18.59 - 29.3

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.

13

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: 2024-06-24 / 2024-06-24

Ссылки на источник:

- http://git.savannah.gnu.org/cgit/emacs.git/tree/etc/NEWS?h=emacs-29
- http://list.orgmode.org/87sex5gdqc.fsf%40localhost/
- http://lists.gnu.org/archive/html/info-gnu-emacs/2024-06/msg00000.html
- http://git.savannah.gnu.org/cgit/emacs/org-mode.git/commit/?id=f4cc61636947b5c2f0afc67174dd369fe3277aa8
- http://www.openwall.com/lists/oss-security/2024/06/23/1
- http://www.openwall.com/lists/oss-security/2024/06/23/2
- http://news.ycombinator.com/item?id=40768225
- https://bdu.fstec.ru/vul/2024-04783