

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2024-08-12.1 | 12 августа 2024 года

TLP: WHITE



Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-42005	Django	Сетевой	ACE	2024-08-07	✓
2	Высокая	CVE-2024-41991	Django	Сетевой	DoS	2024-08-07	✓
3	Высокая	CVE-2024-41990	Django	Сетевой	DoS	2024-08-07	✓
4	Высокая	CVE-2024-41989	Django	Сетевой	DoS	2024-08-07	✓
5	Высокая	CVE-2024-6820	IrfanView	Локальный	ACE	2024-08-07	✓
6	Высокая	CVE-2024-6816	IrfanView	Локальный	ACE	2024-08-07	✓
7	Высокая	CVE-2024-6819	IrfanView	Локальный	ACE	2024-08-07	✓
8	Высокая	CVE-2024-6815	IrfanView	Локальный	ACE	2024-08-07	✓
9	Высокая	CVE-2024-6821	IrfanView	Локальный	ACE	2024-08-07	✓
10	Высокая	CVE-2024-6822	IrfanView	Локальный	ACE	2024-08-07	✓
11	Высокая	CVE-2024-6818	IrfanView	Локальный	ACE	2024-08-07	✓
12	Высокая	CVE-2024-6812	IrfanView	Локальный	ACE	2024-08-07	✓
13	Высокая	CVE-2024-6811	IrfanView	Локальный	ACE	2024-08-07	✓

14	Высокая	CVE-2024-7536	Google Chrome	Сетевой	ACE	2024-08-06	✓
15	Высокая	CVE-2024-7535	Google Chrome	Сетевой	OSI	2024-08-06	✓
16	Высокая	CVE-2024-7534	Google Chrome	Сетевой	ACE	2024-08-06	✓
17	Высокая	CVE-2024-7550	Google Chrome	Сетевой	ACE	2024-08-06	✓
18	Высокая	CVE-2024-7533	Google Chrome	Сетевой	ACE	2024-08-06	✓
19	Высокая	CVE-2024-7532	Google Chrome	Сетевой	ACE	2024-08-06	✓
20	Высокая	CVE-2024-6778	Google Chrome	Сетевой	ACE	2024-08-07	✓
21	Высокая	CVE-2024-7510	Trimble SketchUp, SketchUp Pro and SketchUp Viewer	Локальный	ACE	2024-08-06	✓
22	Высокая	CVE-2024-7509	Trimble SketchUp, SketchUp Pro and SketchUp Viewer	Локальный	ACE	2024-08-06	✓
23	Высокая	CVE-2024-7508	Trimble SketchUp, SketchUp Pro and SketchUp Viewer	Локальный	ACE	2024-08-06	✓
24	Критическая	CVE-2024-38856	Apache OFBiz	Сетевой	ACE	2024-08-06	✓
25	Критическая	CVE-2024-37287	Kibana	Сетевой	ACE	2024-08-06	✓
26	Высокая	CVE-2024-7529	Mozilla Thunderbird	Сетевой	SB	2024-08-07	✓
27	Критическая	CVE-2024-7528	Mozilla Thunderbird	Сетевой	ACE	2024-08-07	✓

28	Высокая	CVE-2024-7527	Mozilla Thunderbird	Сетевой	ACE	2024-08-07	✓
29	Высокая	CVE-2024-7526	Mozilla Thunderbird	Сетевой	SB	2024-08-07	✓
30	Критическая	CVE-2024-7525	Mozilla Thunderbird	Сетевой	SB	2024-08-07	✓
31	Критическая	CVE-2024-7522	Mozilla Thunderbird	Сетевой	ACE	2024-08-07	✓
32	Критическая	CVE-2024-7521	Mozilla Thunderbird	Сетевой	ACE	2024-08-07	✓
33	Высокая	CVE-2024-7520	Mozilla Thunderbird	Сетевой	ACE	2024-08-07	✓
34	Высокая	CVE-2024-7519	Mozilla Thunderbird	Сетевой	ACE	2024-08-07	✓
35	Критическая	CVE-2024-41110	Docker	Сетевой	PE	2024-08-03	✓

Краткое описание: Выполнение произвольного кода в Django

Идентификатор уязвимости: CVE-2024-42005

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

Уязвимый продукт: Django: с версии 4.2 по 5.0.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

1

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

Оценка CVSSv3: 9.8 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: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.djangoproject.com/weblog/2024/aug/06/security-releases/>

Краткое описание: Отказ в обслуживании в Django

Идентификатор уязвимости: CVE-2024-41991

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Django: с версии 4.2 по 5.0.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

2

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: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.djangoproject.com/weblog/2024/aug/06/security-releases/>

Краткое описание: Отказ в обслуживании в Django

Идентификатор уязвимости: CVE-2024-41990

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Django: с версии 4.2 по 5.0.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

3

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: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.djangoproject.com/weblog/2024/aug/06/security-releases/>

Краткое описание: Отказ в обслуживании в Django

Идентификатор уязвимости: CVE-2024-41989

Идентификатор программной ошибки: CWE-400 Неконтролируемое использование ресурсов (исчерпание ресурсов)

Уязвимый продукт: Django: с версии 4.2 по 5.0.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

- 4 **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: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.djangoproject.com/weblog/2024/aug/06/security-releases/>

Краткое описание: Выполнение произвольного кода в IrfanView

Идентификатор уязвимости: CVE-2024-6820

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: IrfanView: с версии 4.00 по 4.66

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-972/>

Краткое описание: Выполнение произвольного кода в IrfanView

Идентификатор уязвимости: CVE-2024-6816

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

Уязвимый продукт: IrfanView: с версии 4.00 по 4.66

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

- 6 **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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-968/>

Краткое описание: Выполнение произвольного кода в IrfanView

Идентификатор уязвимости: CVE-2024-6819

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: IrfanView: с версии 4.00 по 4.66

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-971/>

Краткое описание: Выполнение произвольного кода в IrfanView

Идентификатор уязвимости: CVE-2024-6815

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: IrfanView: с версии 4.00 по 4.66

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

- 8 **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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-967/>

Краткое описание: Выполнение произвольного кода в IrfanView

Идентификатор уязвимости: CVE-2024-6821

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: IrfanView: с версии 4.00 по 4.66

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-973/>

Краткое описание: Выполнение произвольного кода в IrfanView

Идентификатор уязвимости: CVE-2024-6822

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: IrfanView: с версии 4.00 по 4.66

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-974/>

Краткое описание: Выполнение произвольного кода в IrfanView

Идентификатор уязвимости: CVE-2024-6818

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: IrfanView: с версии 4.00 по 4.66

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-970/>

Краткое описание: Выполнение произвольного кода в IrfanView

Идентификатор уязвимости: CVE-2024-6812
BDU:2024-05846

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: IrfanView: с версии 4.00 по 4.66

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-904/>
- <https://bdu.fstec.ru/vul/2024-05846>

Краткое описание: Выполнение произвольного кода в IrfanView

Идентификатор уязвимости: CVE-2024-6811
BDU:2024-05759

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: IrfanView: с версии 4.00 по 4.66

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-903/>
- <https://bdu.fstec.ru/vul/2024-05759>

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7536

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 127.0.6533.90

Категория уязвимого продукта: Прикладное программное обеспечение

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

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: 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: 2024-08-06 / 2024-08-06

Ссылки на источник:

- <http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop.html>
- <http://crbug.com/354847246>

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2024-7535

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 127.0.6533.90

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

15

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:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-06 / 2024-08-06

Ссылки на источник:

- <http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop.html>
- <http://crbug.com/352690885>

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7534

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

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 127.0.6533.90

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-06 / 2024-08-06

Ссылки на источник:

- <http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop.html>
- <http://crbug.com/352467338>

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7550

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

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 127.0.6533.90

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

17

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:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-06 / 2024-08-06

Ссылки на источник:

- <http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop.html>
- <http://crbug.com/355256380>

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7533

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 127.0.6533.90

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

18

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: 2024-08-06 / 2024-08-06

Ссылки на источник:

- <http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop.html>
- <http://crbug.com/353552540>

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-7532

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: с версии 100.0.4896.60 по 127.0.6533.90

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

19

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:N/A:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-06 / 2024-08-06

Ссылки на источник:

- <http://chromereleases.googleblog.com/2024/08/stable-channel-update-for-desktop.html>
- <http://crbug.com/350528343>

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2024-6778
BDU:2024-06114

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

Уязвимый продукт: Google Chrome: до версии 120.0.6099.319

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

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

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: 8.8 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: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://chromereleases.googleblog.com/2024/08/long-term-support-channel-update-for.html>
- <https://bdu.fstec.ru/vul/2024-06114>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp, SketchUp Pro and SketchUp Viewer

Идентификатор уязвимости: CVE-2024-7510

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: SketchUp Desktop: до версии 24.0.553

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-06 / 2024-08-06

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1056/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp, SketchUp Pro and SketchUp Viewer

Идентификатор уязвимости: CVE-2024-7509

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: SketchUp Desktop: до версии 24.0.553

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

22 **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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-06 / 2024-08-06

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1055/>

Краткое описание: Выполнение произвольного кода в Trimble SketchUp, SketchUp Pro and SketchUp Viewer

Идентификатор уязвимости: CVE-2024-7508

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

Уязвимый продукт: SketchUp Viewer:
SketchUp Viewer для Windows: до версии 24.0.553
SketchUp Viewer для Mac: до версии 24.0.553

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:N/I:N/A:H

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-06 / 2024-08-06

Ссылки на источник:

- <http://www.zerodayinitiative.com/advisories/ZDI-24-1054/>

Краткое описание: Выполнение произвольного кода в Apache OFBiz

Идентификатор уязвимости: CVE-2024-38856

BDU:2024-05995

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: OFBiz: с версии 4.0 по 22.01.01

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2024-08-06 / 2024-08-06

Ссылки на источник:

- <http://lists.apache.org/thread/olxxjk6b13sl3wh9cmp0k2dscvp24l7w>
- <http://issues.apache.org/jira/browse/OFBIZ-13128>
- <http://github.com/apache/ofbiz-framework/commit/31d8d7>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1099/>
- <https://bdu.fstec.ru/vul/2024-05995>

Краткое описание: Выполнение произвольного кода в Kibana

Идентификатор уязвимости: CVE-2024-37287
BDU:2024-06005

Идентификатор программной ошибки: CWE-1321 Некорректный контроль за изменениями атрибутов прототипа объекта (Подмена прототипа)

Уязвимый продукт: Kibana: с версии 7.0.0 по 8.14.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

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: 9.9 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: 2024-08-06 / 2024-08-06

Ссылки на источник:

- <http://discuss.elastic.co/t/kibana-8-14-2-7-17-23-security-update-esa-2024-22/364424>
- <https://bdu.fstec.ru/vul/2024-06005>

Краткое описание: Обход безопасности в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-7529

Идентификатор программной ошибки: CWE-450 Наличие вариантов интерпретации входных данных интерфейсом

Уязвимый продукт: Mozilla Thunderbird: версии 128.0
Mozilla Thunderbird: с версии 115.0 по 115.13.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Обход безопасности

- 26 **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: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-37/>

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-7528

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Thunderbird: версии 128.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-37/>

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-7527

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Thunderbird: версии 128.0
Mozilla Thunderbird: с версии 115.0 по 115.13.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 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: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-37/>

Краткое описание: Обход безопасности в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-7526

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Mozilla Thunderbird: версии 128.0
Mozilla Thunderbird: с версии 115.0 по 115.13.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 8.8 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: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-37/>

Краткое описание: Обход безопасности в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-7525

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

Уязвимый продукт: Mozilla Thunderbird: версии 128.0
Mozilla Thunderbird: с версии 115.0 по 115.13.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-37/>

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-7522

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Mozilla Thunderbird: версии 128.0
Mozilla Thunderbird: с версии 115.0 по 115.13.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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: 9.1 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: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-37/>

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-7521

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Thunderbird: версии 128.0
Mozilla Thunderbird: с версии 115.0 по 115.13.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-37/>

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-7520

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

Уязвимый продукт: Mozilla Thunderbird: версии 128.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-37/>

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2024-7519

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Mozilla Thunderbird: версии 128.0
Mozilla Thunderbird: с версии 115.0 по 115.13.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2024-08-07 / 2024-08-07

Ссылки на источник:

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-37/>

Краткое описание: Повышение привилегий в Docker

Идентификатор уязвимости: CVE-2024-41110
BDU:2024-05760

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: Docker Engine:
до версии 18.09.1
с версии 19.03 до версии 19.03.15
с версии 20.10 до версии 20.10.27
с версии 23.0 до версии 23.0.14
с версии 24.0.0 до версии 24.0.9
с версии 25.0.5 до версии 25.0.5
с версии 26.0.0 до версии 26.0.2
с версии 27.0.0 до версии 27.0.3
до версии 27.1.1
с версии 26.1.4 до версии 26.1.4

35

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

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: 9.9 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: 2024-08-03 / 2024-08-03

Ссылки на источник:

- <https://bdu.fstec.ru/vul/2024-05760>