

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](https://cert.gov.ru)

E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

## Бюллетень об уязвимостях программного обеспечения

VULN.2024-10-07.1 | 7 октября 2024 года

TLP: WHITE



## Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-9402	Mozilla	Сетевой	ACE	2024-10-01	✓
2	Критическая	CVE-2024-9401	Mozilla	Сетевой	ACE	2024-10-01	✓
3	Высокая	CVE-2024-9400	Mozilla	Сетевой	DoS	2024-10-01	✓
4	Высокая	CVE-2024-9396	Mozilla	Сетевой	ACE	2024-10-01	✓
5	Высокая	CVE-2024-9394	Mozilla	Сетевой	SB	2024-10-01	✓
6	Высокая	CVE-2024-9393	Mozilla	Сетевой	SB	2024-10-01	✓
7	Критическая	CVE-2024-9392	Mozilla	Сетевой	ACE	2024-10-01	✓
8	Критическая	CVE-2024-9370	Google Chrome	Сетевой	OSI	2024-10-02	✓
9	Критическая	CVE-2024-9369	Google Chrome	Сетевой	ACE	2024-10-02	✓
10	Критическая	CVE-2024-7025	Google Chrome	Сетевой	ACE	2024-10-02	✓
11	Высокая	CVE-2024-7723	Foxit PDF Reader and Editor for Windows	Локальный	ACE	2024-10-01	✓
12	Высокая	CVE-2024-7724	Foxit PDF Reader and Editor for Windows	Локальный	ACE	2024-10-01	✓
13	Высокая	CVE-2024-7725	Foxit PDF Reader and Editor	Локальный	ACE	2024-10-01	✓

14	Критическая	CVE-2024-9243	Foxit PDF Reader and Editor	Сетевой	ACE	2024-10-01	✓
15	Критическая	CVE-2024-9246	Foxit PDF Reader and Editor for Windows	Сетевой	ACE	2024-10-01	✓
16	Высокая	CVE-2024-9250	Foxit PDF Reader and Editor for Windows	Сетевой	ACE	2024-10-01	✓
17	Критическая	CVE-2024-9252	Foxit PDF Reader and Editor for Windows	Сетевой	ACE	2024-10-01	✓
18	Критическая	CVE-2024-9253	Foxit PDF Reader and Editor for Windows	Сетевой	ACE	2024-10-01	✓
19	Критическая	CVE-2024-9251	Foxit PDF Reader and Editor for Windows	Сетевой	ACE	2024-10-01	✓
20	Высокая	CVE-2024-28888	Foxit PDF Reader and Editor	Сетевой	ACE	2024-10-01	✓
21	Критическая	CVE-2024-9254	Foxit PDF Reader and Editor	Сетевой	ACE	2024-10-01	✓
22	Критическая	CVE-2024-9256	Foxit PDF Reader and Editor for Windows	Сетевой	ACE	2024-10-01	✓
23	Высокая	CVE-2024-9245	Foxit PDF Reader and Editor for Windows	Локальный	ACE	2024-10-01	✓
24	Высокая	CVE-2024-9244	Foxit PDF Reader and Editor for Windows	Локальный	ACE	2024-10-01	✓
25	Высокая	CVE-2024-38393	Foxit PDF Reader and Editor for Windows	Локальный	ACE	2024-10-01	✓
26	Критическая	CVE-2024-9247	Foxit PDF Reader and Editor for Windows	Сетевой	ACE	2024-10-01	✓

27	Критическая	CVE-2024-9249	Foxit PDF Reader and Editor for Windows	Сетевой	ACE	2024-10-01	✓
28	Критическая	CVE-2024-9248	Foxit PDF Reader and Editor for Windows	Сетевой	ACE	2024-10-01	✓
29	Высокая	CVE-2024-41605	Foxit PDF Reader and Editor for Windows	Локальный	PE	2024-10-01	✓
30	Высокая	CVE-2024-9255	Foxit PDF Reader and Editor for Windows	Локальный	ACE	2024-10-01	✓
31	Высокая	CVE-2024-7675	Autodesk Navisworks	Локальный	ACE	2024-10-01	✓
32	Высокая	CVE-2024-7674	Autodesk Navisworks	Локальный	ACE	2024-10-01	✓
33	Высокая	CVE-2024-7673	Autodesk Navisworks	Локальный	ACE	2024-10-01	✓
34	Высокая	CVE-2024-7672	Autodesk Navisworks	Локальный	ACE	2024-10-01	✓
35	Высокая	CVE-2024-7671	Autodesk Navisworks	Локальный	ACE	2024-10-01	✓
36	Высокая	CVE-2024-7670	Autodesk Navisworks	Локальный	OSI	2024-10-01	✓
37	Критическая	CVE-2024-46908	WhatsUp Gold	Сетевой	ACE	2024-10-01	✓
38	Высокая	CVE-2024-45408	eLabFTW	Сетевой	OSI	2024-10-02	✓
39	Высокая	CVE-2024-25632	eLabFTW	Сетевой	PE	2024-10-02	✓
40	Высокая	CVE-2024-45294	HL7 fhir-ig-publisher	Сетевой	OSI	2024-10-02	✓

41	Критическая	CVE-2024-45367	Optigo Networks ONS-S8 Spectra Aggregation Switch	Сетевой	SB	2024-10-02	✗
42	Критическая	CVE-2024-41925	Optigo Networks ONS-S8 Spectra Aggregation Switch	Сетевой	ACE	2024-10-02	✗
43	Высокая	CVE-2024-47136	JTEKT ELECTRONICS Kostac PLC Programming Software	Локальный	OSI	2024-10-02	✓
44	Высокая	CVE-2024-47135	JTEKT ELECTRONICS Kostac PLC Programming Software	Локальный	ACE	2024-10-02	✓
45	Высокая	CVE-2024-47134	JTEKT ELECTRONICS Kostac PLC Programming Software	Локальный	ACE	2024-10-02	✓
46	Критическая	CVE-2024-20432	Cisco Nexus Dashboard Fabric Controller (NDFC)	Сетевой	ACE	2024-10-04	✗
47	Высокая	CVE-2024-20449	Cisco Nexus Dashboard Fabric Controller (NDFC)	Сетевой	ACE	2024-10-04	✗
48	Высокая	CVE-2024-20393	Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers	Сетевой	PE	2024-10-04	✗
49	Высокая	CVE-2024-3596	Juniper Junos OS and Junos OS Evolved	Сетевой	OSI	2024-10-03	✗
50	Высокая	CVE-2024-20501	Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices	Сетевой	DoS	2024-10-04	✓
51	Высокая	CVE-2024-20499	Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices	Сетевой	DoS	2024-10-04	✓
52	Высокая	CVE-2024-20498	Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices	Сетевой	DoS	2024-10-04	✓

53	Критическая	CVE-2024-47561	Apache Avro	Сетевой	ACE	2024-10-03	✓
54	Критическая	CVE-2024-38526	mitmproxy pdoc	Сетевой	ACE	2024-10-03	✓
55	Критическая	CVE-2024-41592	DrayTek products	Сетевой	ACE	2024-10-03	✓
56	Высокая	CVE-2024-41585	DrayTek products	Локальный	ACE	2024-10-03	✓
57	Высокая	CVE-2024-41589	DrayTek products	Смежная сеть	OSI	2024-10-03	✓
58	Критическая	CVE-2024-47177	Google ChromeOS LTS	Сетевой	ACE	2024-10-03	✓
59	Высокая	CVE-2024-47175	Google ChromeOS LTS	Сетевой	OSI	2024-10-03	✓
60	Высокая	CVE-2024-47076	Google ChromeOS LTS	Сетевой	OSI	2024-10-03	✓

**Краткое описание:** Выполнение произвольного кода в Mozilla

**Идентификатор уязвимости:** CVE-2024-9402

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

**Уязвимый продукт:** Mozilla Firefox: 100.0 - 130.0.1  
Firefox for Android: 100.1.0 - 130.0.1  
Firefox ESR: 102.0 - 128.2.0  
Mozilla Thunderbird: 13.0.1 - 130.0  
Mozilla Thunderbird: 128.0 - 128.2.3

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <https://www.mozilla.org/security/advisories/mfsa2024-50/>
- <https://www.mozilla.org/security/advisories/mfsa2024-49/>
- <https://www.mozilla.org/security/advisories/mfsa2024-48/>
- <https://www.mozilla.org/security/advisories/mfsa2024-47/>
- <https://www.mozilla.org/security/advisories/mfsa2024-46/>

**Краткое описание:** Выполнение произвольного кода в Mozilla

**Идентификатор уязвимости:** CVE-2024-9401

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

**Уязвимый продукт:** Mozilla Firefox: 100.0 - 130.0.1  
Firefox for Android: 100.1.0 - 130.0.1  
Firefox ESR: 102.0 - 128.2.0  
Mozilla Thunderbird: 13.0.1 - 130.0  
Mozilla Thunderbird: 128.0 - 128.2.3

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Выполнение произвольного кода

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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <https://www.mozilla.org/security/advisories/mfsa2024-50/>
- <https://www.mozilla.org/security/advisories/mfsa2024-49/>
- <https://www.mozilla.org/security/advisories/mfsa2024-48/>
- <https://www.mozilla.org/security/advisories/mfsa2024-47/>
- <https://www.mozilla.org/security/advisories/mfsa2024-46/>

**Краткое описание:** Отказ в обслуживании в Mozilla

**Идентификатор уязвимости:** CVE-2024-9400

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

**Уязвимый продукт:** Mozilla Firefox: 100.0 - 130.0.1  
Firefox for Android: 100.1.0 - 130.0.1  
Firefox ESR: 102.0 - 128.2.0  
Mozilla Thunderbird: 13.0.1 - 130.0  
Mozilla Thunderbird: 128.0 - 128.2.3

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Не определено

**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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <https://www.mozilla.org/security/advisories/mfsa2024-50/>
- <https://www.mozilla.org/security/advisories/mfsa2024-49/>
- <https://www.mozilla.org/security/advisories/mfsa2024-48/>
- <https://www.mozilla.org/security/advisories/mfsa2024-47/>
- <https://www.mozilla.org/security/advisories/mfsa2024-46/>

**Краткое описание:** Выполнение произвольного кода в Mozilla

**Идентификатор уязвимости:** CVE-2024-9396

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

**Уязвимый продукт:** Mozilla Firefox: 100.0 - 130.0.1  
Firefox for Android: 100.1.0 - 130.0.1  
Firefox ESR: 102.0 - 128.2.0  
Mozilla Thunderbird: 13.0.1 - 130.0  
Mozilla Thunderbird: 128.0 - 128.2.3

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Выполнение произвольного кода

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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <https://www.mozilla.org/security/advisories/mfsa2024-50/>
- <https://www.mozilla.org/security/advisories/mfsa2024-49/>
- <https://www.mozilla.org/security/advisories/mfsa2024-48/>
- <https://www.mozilla.org/security/advisories/mfsa2024-47/>
- <https://www.mozilla.org/security/advisories/mfsa2024-46/>

**Краткое описание:** Обход безопасности в Mozilla

**Идентификатор уязвимости:** CVE-2024-9394

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

**Уязвимый продукт:** Mozilla Firefox: 100.0 - 130.0.1  
Firefox for Android: 100.1.0 - 130.0.1  
Firefox ESR: 102.0 - 128.2.0  
Mozilla Thunderbird: 13.0.1 - 130.0  
Mozilla Thunderbird: 128.0 - 128.2.3

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Обход безопасности

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <https://www.mozilla.org/security/advisories/mfsa2024-50/>
- <https://www.mozilla.org/security/advisories/mfsa2024-49/>
- <https://www.mozilla.org/security/advisories/mfsa2024-48/>
- <https://www.mozilla.org/security/advisories/mfsa2024-47/>
- <https://www.mozilla.org/security/advisories/mfsa2024-46/>

**Краткое описание:** Обход безопасности в Mozilla

**Идентификатор уязвимости:** CVE-2024-9393

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

**Уязвимый продукт:** Mozilla Firefox: 100.0 - 130.0.1  
Firefox for Android: 100.1.0 - 130.0.1  
Firefox ESR: 102.0 - 128.2.0  
Mozilla Thunderbird: 13.0.1 - 130.0  
Mozilla Thunderbird: 128.0 - 128.2.3

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Обход безопасности

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <https://www.mozilla.org/security/advisories/mfsa2024-50/>
- <https://www.mozilla.org/security/advisories/mfsa2024-49/>
- <https://www.mozilla.org/security/advisories/mfsa2024-48/>
- <https://www.mozilla.org/security/advisories/mfsa2024-47/>
- <https://www.mozilla.org/security/advisories/mfsa2024-46/>

**Краткое описание:** Выполнение произвольного кода в Mozilla

**Идентификатор уязвимости:** CVE-2024-9392

**Идентификатор программной ошибки:** CWE-254 Уязвимости в безопасности ПО

**Уязвимый продукт:** Mozilla Firefox: 100.0 - 130.0.1  
Firefox for Android: 100.1.0 - 130.0.1  
Firefox ESR: 102.0 - 128.2.0  
Mozilla Thunderbird: 13.0.1 - 130.0  
Mozilla Thunderbird: 128.0 - 128.2.3

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Обход ограничений безопасности

**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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <https://www.mozilla.org/security/advisories/mfsa2024-50/>
- <https://www.mozilla.org/security/advisories/mfsa2024-49/>
- <https://www.mozilla.org/security/advisories/mfsa2024-48/>
- <https://www.mozilla.org/security/advisories/mfsa2024-47/>
- <https://www.mozilla.org/security/advisories/mfsa2024-46/>

**Краткое описание:** Получение конфиденциальной информации в Google Chrome

**Идентификатор уязвимости:** CVE-2024-9370

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

**Уязвимый продукт:** Google Chrome: с версии 100.0.4896.60 по 129.0.6668.72

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Получение конфиденциальной информации

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:** 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:** 2024-10-02 / 2024-10-02

**Ссылки на источник:**

- <http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop.html>
- <http://crbug.com/368311899>

**Краткое описание:** Выполнение произвольного кода в Google Chrome

**Идентификатор уязвимости:** CVE-2024-9369

**Идентификатор программной ошибки:** CWE-20 Некорректная проверка входных данных

**Уязвимый продукт:** Google Chrome: с версии 100.0.4896.60 по 129.0.6668.72

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**Последствия эксплуатации:** Выполнение произвольного кода

9

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

**Оценка CVSSv3:** 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-02 / 2024-10-02

**Ссылки на источник:**

- <http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop.html>
- <http://crbug.com/368208152>

**Краткое описание:** Выполнение произвольного кода в Google Chrome

**Идентификатор уязвимости:** CVE-2024-7025

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

**Уязвимый продукт:** Google Chrome: с версии 100.0.4896.60 по 129.0.6668.72

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

**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:** 2024-10-02 / 2024-10-02

**Ссылки на источник:**

- <http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop.html>
- <http://crbug.com/367764861>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-7723

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.7.15526

**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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-7724  
BDU:2024-06550

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.7.15526

**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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <https://bdu.fstec.ru/vul/2024-06550>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor

**Идентификатор уязвимости:** CVE-2024-7725

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 12.1.7.15526  
Foxit PDF Editor for Mac (formerly PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**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:HI/H/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor

**Идентификатор уязвимости:** CVE-2024-9243

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402  
Foxit PDF Editor for Mac (formerly PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1296/>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-9246

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Выполнение произвольного кода

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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1299/>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-9250

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1303/>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-9252

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1304/>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-9253

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1305/>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-9251

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1306/>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor

**Идентификатор уязвимости:** CVE-2024-28888

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402  
Foxit PDF Editor for Mac (formerly PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- [http://www.talosintelligence.com/vulnerability\\_reports/TALOS-2024-1967](http://www.talosintelligence.com/vulnerability_reports/TALOS-2024-1967)

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor

**Идентификатор уязвимости:** CVE-2024-9254

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402  
Foxit PDF Editor for Mac (formerly PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1307/>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-9256

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1309/>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-9245

**Идентификатор программной ошибки:** CWE-426 Подмена пути исполнения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

23 **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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1297/>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-9244

**Идентификатор программной ошибки:** CWE-426 Подмена пути исполнения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

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:** 7.8 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1298/>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-38393

**Идентификатор программной ошибки:** CWE-426 Подмена пути исполнения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально сформированных 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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-9247

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Выполнение произвольного кода

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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1300/>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-9249

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1301/>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-9248

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**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:** 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1302/>

**Краткое описание:** Повышение привилегий в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-41605  
BDU:2024-07681

**Идентификатор программной ошибки:** CWE-354 Некорректная проверка контрольных сумм

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Выполнение специально созданного вредоносного файла

**Последствия эксплуатации:** Повышение привилегий

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <https://bdu.fstec.ru/vul/2024-07681>

**Краткое описание:** Выполнение произвольного кода в Foxit PDF Reader and Editor for Windows

**Идентификатор уязвимости:** CVE-2024-9255

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Foxit PDF Reader for Windows: с версии 11.0.0.49893 по 2024.2.3.25184  
Foxit PDF Editor (formerly Foxit PhantomPDF): с версии 11.0.0.0510 по 2024.2.3.64402

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Выполнение произвольного кода

30

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

**Оценка CVSSv3:** 7.8 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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://www.foxitsoftware.com/support/security-bulletins.html>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1308/>

Краткое описание: Выполнение произвольного кода в Autodesk Navisworks

Идентификатор уязвимости: CVE-2024-7675

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Autodesk Navisworks: 2025

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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: 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: 2024-10-01 / 2024-10-01

Ссылки на источник:

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0015>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1315/>

Краткое описание: Выполнение произвольного кода в Autodesk Navisworks

Идентификатор уязвимости: CVE-2024-7674

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

Уязвимый продукт: Autodesk Navisworks: 2025

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-10-01 / 2024-10-01

Ссылки на источник:

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0015>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1320/>

Краткое описание: Выполнение произвольного кода в Autodesk Navisworks

Идентификатор уязвимости: CVE-2024-7673

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

Уязвимый продукт: Autodesk Navisworks: 2025

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-10-01 / 2024-10-01

Ссылки на источник:

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0015>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1316/>

Краткое описание: Выполнение произвольного кода в Autodesk Navisworks

Идентификатор уязвимости: CVE-2024-7672

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk Navisworks: 2025

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 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: 2024-10-01 / 2024-10-01

Ссылки на источник:

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0015>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1319/>

Краткое описание: Выполнение произвольного кода в Autodesk Navisworks

Идентификатор уязвимости: CVE-2024-7671

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Autodesk Navisworks: 2025

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

35

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: 2024-10-01 / 2024-10-01

Ссылки на источник:

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0015>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1318/>

Краткое описание: Получение конфиденциальной информации в Autodesk Navisworks

Идентификатор уязвимости: CVE-2024-7670

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Autodesk Navisworks: 2025

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

36

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: 2024-10-01 / 2024-10-01

Ссылки на источник:

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0015>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1317/>

**Краткое описание:** Выполнение произвольного кода в WhatsUp Gold

**Идентификатор уязвимости:** CVE-2024-46908

**Идентификатор программной ошибки:** CWE-20 Некорректная проверка входных данных

**Уязвимый продукт:** WhatsUp Gold: до версии 24.0.1

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

37 **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:** 2024-10-01 / 2024-10-01

**Ссылки на источник:**

- <http://community.progress.com/s/article/WhatsUp-Gold-Security-Bulletin-September-2024>

**Краткое описание:** Получение конфиденциальной информации в eLabFTW

**Идентификатор уязвимости:** CVE-2024-45408

**Идентификатор программной ошибки:** CWE-284 Некорректное управление доступом

**Уязвимый продукт:** eLabFTW: 4.4.1 - 5.0.4

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Обход ограничений безопасности

**Последствия эксплуатации:** Получение конфиденциальной информации

38

**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:** 2024-10-02 / 2024-10-02

**Ссылки на источник:**

- <http://github.com/elabftw/elabftw/security/advisories/GHSA-2c83-6j74-w8r5>

Краткое описание: Повышение привилегий в eLabFTW

Идентификатор уязвимости: CVE-2024-25632

Идентификатор программной ошибки: CWE-266 Некорректное назначение привилегий

Уязвимый продукт: eLabFTW: 4.6.0 - 5.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Повышение привилегий

39 **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:H/I:L/A:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-10-02 / 2024-10-02

Ссылки на источник:

- <http://github.com/elabftw/elabftw/security/advisories/GHSA-6m7p-gh9f-5mgg>

**Краткое описание:** Получение конфиденциальной информации в HL7 fhir-ig-publisher

**Идентификатор уязвимости:** CVE-2024-45294

**Идентификатор программной ошибки:** CWE-611 Некорректное ограничение ссылок на внешние сущности XML

**Уязвимый продукт:** fhir-ig-publisher: 1.1.0 - 1.6.21

**Категория уязвимого продукта:** Универсальные компоненты и библиотеки

**Способ эксплуатации:** Отправка специально созданного вредоносного XML-кода.

**Последствия эксплуатации:** Получение конфиденциальной информации

40

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

**Оценка CVSSv3:** 8.6 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-02 / 2024-10-02

**Ссылки на источник:**

- <http://github.com/HL7/fhir-ig-publisher/security/advisories/GHSA-59rq-22fm-x8q5>
- <http://github.com/HL7/fhir-ig-publisher/releases/tag/1.6.22>

Краткое описание: Обход безопасности в Optigo Networks ONS-S8 Spectra Aggregation Switch

Идентификатор уязвимости: CVE-2024-45367

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: ONS-S8 - Spectra Aggregation Switch: 1.3.7

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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

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: 2024-10-02 / 2024-10-02

Ссылки на источник:

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-275-01>

**Краткое описание:** Выполнение произвольного кода в Optigo Networks ONS-S8 Spectra Aggregation Switch

**Идентификатор уязвимости:** CVE-2024-41925

**Идентификатор программной ошибки:** CWE-98 Уязвимости, связанные с именами файлов для PHP-функций include или require (удаленное внедрение файлов в PHP)

**Уязвимый продукт:** ONS-S8 - Spectra Aggregation Switch: 1.3.7

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально созданных HTTP-запросов.

**Последствия эксплуатации:** Выполнение произвольного кода

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

**Оценка CVSSv3:** 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-02 / 2024-10-02

**Ссылки на источник:**

- <http://www.cisa.gov/news-events/ics-advisories/icsa-24-275-01>

**Краткое описание:** Получение конфиденциальной информации в JTEKT ELECTRONICS Kostac PLC Programming Software

**Идентификатор уязвимости:** CVE-2024-47136

**Идентификатор программной ошибки:** CWE-125 Чтение за пределами буфера

**Уязвимый продукт:** Kostac PLC Programming Software: 1.6.14.0

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Получение конфиденциальной информации

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:** 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:** 2024-10-02 / 2024-10-02

**Ссылки на источник:**

- <http://jvn.jp/en/vu/JVNVU92808077/index.html>

**Краткое описание:** Выполнение произвольного кода в JTEKT ELECTRONICS Kostac PLC Programming Software

**Идентификатор уязвимости:** CVE-2024-47135

**Идентификатор программной ошибки:** CWE-121 Переполнение буфера в стеке

**Уязвимый продукт:** Kostac PLC Programming Software: 1.6.14.0

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Выполнение произвольного кода

44 **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:** 2024-10-02 / 2024-10-02

**Ссылки на источник:**

- <http://jvn.jp/en/vu/JVNVU92808077/index.html>

**Краткое описание:** Выполнение произвольного кода в JTEKT ELECTRONICS Kostac PLC Programming Software

**Идентификатор уязвимости:** CVE-2024-47134

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** Kostac PLC Programming Software: 1.6.14.0

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

**Последствия эксплуатации:** Выполнение произвольного кода

45

**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:** 2024-10-02 / 2024-10-02

**Ссылки на источник:**

- <http://jvn.jp/en/vu/JVNVU92808077/index.html>

**Краткое описание:** Выполнение произвольного кода в Cisco Nexus Dashboard Fabric Controller (NDFC)

**Идентификатор уязвимости:** CVE-2024-20432  
BDU:2024-07739

**Идентификатор программной ошибки:** CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

**Уязвимый продукт:** Cisco Nexus Dashboard Fabric Controller (NDFC): 12.0

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-04 / 2024-10-04

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-cmdinj-UvYZrKfr>
- <https://bdu.fstec.ru/vul/2024-07739>

**Краткое описание:** Выполнение произвольного кода в Cisco Nexus Dashboard Fabric Controller (NDFC)

**Идентификатор уязвимости:** CVE-2024-20449

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

**Уязвимый продукт:** Cisco Nexus Dashboard Fabric Controller (NDFC): 12.0

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально созданных HTTP-запросов.

**Последствия эксплуатации:** Выполнение произвольного кода

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

**Оценка CVSSv3:** 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-04 / 2024-10-04

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ndfc-ptnce-BUSHLbp>

**Краткое описание:** Повышение привилегий в Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers

**Идентификатор уязвимости:** CVE-2024-20393

**Идентификатор программной ошибки:** CWE-285 Некорректная авторизация

**Уязвимый продукт:** Cisco RV340 Dual WAN Gigabit VPN Router: все версии  
Cisco RV340W Dual WAN Gigabit Wireless-AC VPN Router: все версии  
Cisco RV345 Dual WAN Gigabit VPN Router: все версии  
RV345P Dual WAN Gigabit PoE VPN Router: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально созданного HTTP-запроса.

48

**Последствия эксплуатации:** Повышение привилегий

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

**Оценка CVSSv3:** 8.8 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-04 / 2024-10-04

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv34x-privesc-rce-qE33TCms>

**Краткое описание:** Получение конфиденциальной информации в Juniper Junos OS and Junos OS Evolved

**Идентификатор уязвимости:** CVE-2024-3596  
BDU:2024-05180

**Идентификатор программной ошибки:** CWE-327 Использование скомпрометированного или ненадежного криптографического алгоритма

**Уязвимый продукт:** Juniper Junos OS: 21.4R1 - 23.4R2-S2  
Junos OS Evolved: 21.4R1-EVO - 23.4R2-S2-EVO  
Junos cRPD: до 24.4R1

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

**Способ эксплуатации:** Обход ограничений безопасности

49 **Последствия эксплуатации:** Получение конфиденциальной информации

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

**Оценка CVSSv3:** 7.5 AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-03 / 2024-10-03

**Ссылки на источник:**

- <http://supportportal.juniper.net/s/article/2024-09-30-Out-of-Cycle-Security-Advisory-Multiple-Products-RADIUS-protocol-susceptible-to-forgery-attacks-Blast-RADIUS-CVE-2024-3596>
- <https://bdu.fstec.ru/vul/2024-05180>

**Краткое описание:** Отказ в обслуживании в Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices

**Идентификатор уязвимости:** CVE-2024-20501

**Идентификатор программной ошибки:** CWE-415 Двойное освобождение

**Уязвимый продукт:** Meraki MX: 16.2 - 18.0

Cisco Meraki MX64: все версии  
Cisco Meraki MX64W: все версии  
Cisco Meraki MX65: все версии  
Cisco Meraki MX65W: все версии  
Cisco Meraki MX67: все версии  
Cisco Meraki MX67C: все версии  
Cisco Meraki MX67W: все версии  
Cisco Meraki MX68: все версии  
Cisco Meraki MX68CW: все версии  
Cisco Meraki MX68W: все версии  
Cisco Meraki MX75: все версии  
Cisco Meraki MX84: все версии  
Cisco Meraki MX85: все версии  
Cisco Meraki MX95: все версии  
Cisco Meraki MX100: все версии  
Cisco Meraki MX105: все версии  
Cisco Meraki MX250: все версии  
Cisco Meraki MX400: все версии  
Cisco Meraki MX450: все версии  
Cisco Meraki MX600: все версии  
Cisco Meraki vMX: все версии  
Cisco Meraki Z3: все версии  
Cisco Meraki Z3Z3C: все версии  
Cisco Meraki Z3Z4: все версии  
Cisco Meraki Z3Z4C: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Отказ в обслуживании

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

**Оценка CVSSv3:** 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:** 2024-10-04 / 2024-10-04

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2>

**Краткое описание:** Отказ в обслуживании в Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices

**Идентификатор уязвимости:** CVE-2024-20499

**Идентификатор программной ошибки:** CWE-415 Двойное освобождение

**Уязвимый продукт:** Meraki MX: 16.2 - 18.0

Cisco Meraki MX64: все версии

Cisco Meraki MX64W: все версии

Cisco Meraki MX65: все версии

Cisco Meraki MX65W: все версии

Cisco Meraki MX67: все версии

Cisco Meraki MX67C: все версии

Cisco Meraki MX67W: все версии

Cisco Meraki MX68: все версии

Cisco Meraki MX68CW: все версии

Cisco Meraki MX68W: все версии

Cisco Meraki MX75: все версии

Cisco Meraki MX84: все версии

Cisco Meraki MX85: все версии

Cisco Meraki MX95: все версии

Cisco Meraki MX100: все версии

Cisco Meraki MX105: все версии

Cisco Meraki MX250: все версии

Cisco Meraki MX400: все версии

Cisco Meraki MX450: все версии

Cisco Meraki MX600: все версии

Cisco Meraki vMX: все версии

Cisco Meraki Z3: все версии

Cisco Meraki Z3Z3C: все версии

Cisco Meraki Z3Z4: все версии

Cisco Meraki Z3Z4C: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Отказ в обслуживании

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

**Оценка CVSSv3:** 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:** 2024-10-04 / 2024-10-04

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2>

**Краткое описание:** Отказ в обслуживании в Cisco Meraki MX and Cisco Meraki Z Series Teleworker Gateway devices

**Идентификатор уязвимости:** CVE-2024-20498

**Идентификатор программной ошибки:** CWE-415 Двойное освобождение

**Уязвимый продукт:** Meraki MX: 16.2 - 18.0

Cisco Meraki MX64: все версии

Cisco Meraki MX64W: все версии

Cisco Meraki MX65: все версии

Cisco Meraki MX65W: все версии

Cisco Meraki MX67: все версии

Cisco Meraki MX67C: все версии

Cisco Meraki MX67W: все версии

Cisco Meraki MX68: все версии

Cisco Meraki MX68CW: все версии

Cisco Meraki MX68W: все версии

Cisco Meraki MX75: все версии

Cisco Meraki MX84: все версии

Cisco Meraki MX85: все версии

Cisco Meraki MX95: все версии

Cisco Meraki MX100: все версии

Cisco Meraki MX105: все версии

Cisco Meraki MX250: все версии

Cisco Meraki MX400: все версии

Cisco Meraki MX450: все версии

Cisco Meraki MX600: все версии

Cisco Meraki vMX: все версии

Cisco Meraki Z3: все версии

Cisco Meraki Z3Z3C: все версии

Cisco Meraki Z3Z4: все версии

Cisco Meraki Z3Z4C: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Отказ в обслуживании

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

**Оценка CVSSv3:** 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:** 2024-10-04 / 2024-10-04

**Ссылки на источник:**

- <http://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-meraki-mx-vpn-dos-QTRHzG2>

**Краткое описание:** Выполнение произвольного кода в Apache Avro

**Идентификатор уязвимости:** CVE-2024-47561

**Идентификатор программной ошибки:** CWE-20 Некорректная проверка входных данных

**Уязвимый продукт:** Apache Avro: 1.0.0 - 1.11.3

**Категория уязвимого продукта:** Серверное программное обеспечение и его компоненты

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

53 **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:** 2024-10-03 / 2024-10-03

**Ссылки на источник:**

- <http://lists.apache.org/thread/c2v7mhqnmq0jmbwxqq3r5bj1xg43h5x>

54

**Краткое описание:** Выполнение произвольного кода в mitmproxy pdoc

**Идентификатор уязвимости:** CVE-2024-38526

**Идентификатор программной ошибки:** CWE-506 Внедренный вредоносный код

**Уязвимый продукт:** pdoc: 0.1.0 - 14.5.0

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** Выполнение произвольного кода

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

**Оценка CVSSv3:** 9.6 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:L/E:U/RL:O/RC:C

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-03 / 2024-10-03

**Ссылки на источник:**

- <http://github.com/mitmproxy/pdoc/security/advisories/GHSA-5vgj-ggm4-fg62>
- <http://github.com/mitmproxy/pdoc/pull/703>
- <http://sansec.io/research/polyfill-supply-chain-attack>
- <http://www.vicarius.io/vsociety/posts/polyfillio-in-pdoc-cve-2024-38526>

**Краткое описание:** Выполнение произвольного кода в DrayTek products

**Идентификатор уязвимости:** CVE-2024-41592  
BDU:2024-07740

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

**Уязвимый продукт:** Vigor 1000B: до 4.3.2.8  
Vigor 2962: до 4.3.2.8  
Vigor 3910: до 4.3.2.8  
Vigor 3912: до 4.3.6.1  
Vigor 165: до 4.2.7  
Vigor 166: до 4.2.7  
Vigor 2135: до 4.4.5.1  
Vigor 2763: до 4.4.5.1  
Vigor 2765: до 4.4.5.1  
Vigor 2766: до 4.4.5.1  
Vigor 2865: до 4.4.5.3  
Vigor 2866: до 4.4.5.3  
Vigor 2915: до 4.4.5.3  
Vigor 2620: до 3.9.8.9  
Vigor LTE200: до 3.9.8.9  
Vigor 2133: до 3.9.9  
Vigor 2762: до 3.9.9  
Vigor 2832: до 3.9.9  
Vigor 2860: до 3.9.8  
Vigor 2925: до 3.9.8  
Vigor 2862: до 3.9.9.5  
Vigor 2926: до 3.9.9.5  
Vigor 2952: до 3.9.8.2  
Vigor 3220: до 3.9.8.2

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально созданных HTTP-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:N/A:H/E:U/RL:O/RC:C

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-03 / 2024-10-03

**Ссылки на источник:**

- <http://www.forescout.com/resources/draybreak-draytek-research/>
- <https://bdu.fstec.ru/vul/2024-07740>

**Краткое описание:** Выполнение произвольного кода в DrayTek products

**Идентификатор уязвимости:** CVE-2024-41585

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

**Уязвимый продукт:** Vigor 1000B: до 4.3.2.8  
Vigor 2962: до 4.3.2.8  
Vigor 3910: до 4.3.2.8  
Vigor 3912: до 4.3.6.1  
Vigor 165: до 4.2.7  
Vigor 166: до 4.2.7  
Vigor 2135: до 4.4.5.1  
Vigor 2763: до 4.4.5.1  
Vigor 2765: до 4.4.5.1  
Vigor 2766: до 4.4.5.1  
Vigor 2865: до 4.4.5.3  
Vigor 2866: до 4.4.5.3  
Vigor 2915: до 4.4.5.3  
Vigor 2620: до 3.9.8.9  
Vigor LTE200: до 3.9.8.9  
Vigor 2133: до 3.9.9  
Vigor 2762: до 3.9.9  
Vigor 2832: до 3.9.9  
Vigor 2860: до 3.9.8  
Vigor 2925: до 3.9.8  
Vigor 2862: до 3.9.9.5  
Vigor 2926: до 3.9.9.5  
Vigor 2952: до 3.9.8.2  
Vigor 3220: до 3.9.8.2

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Отправка специально сформированных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

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

**Оценка CVSSv3:** 8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-03 / 2024-10-03

**Ссылки на источник:**

- <http://www.forescout.com/resources/draybreak-draytek-research/>

Краткое описание: Получение конфиденциальной информации в DrayTek products

Идентификатор уязвимости: CVE-2024-41589

Идентификатор программной ошибки: CWE-255 Уязвимости, связанные с управлением учетными данными

Уязвимый продукт: Vigor 1000B: до 4.3.2.8

Vigor 2962: до 4.3.2.8

Vigor 3910: до 4.3.2.8

Vigor 3912: до 4.3.6.1

Vigor 165: до 4.2.7

Vigor 166: до 4.2.7

Vigor 2135: до 4.4.5.1

Vigor 2763: до 4.4.5.1

Vigor 2765: до 4.4.5.1

Vigor 2766: до 4.4.5.1

Vigor 2865: до 4.4.5.3

Vigor 2866: до 4.4.5.3

Vigor 2915: до 4.4.5.3

Vigor 2620: до 3.9.8.9

Vigor LTE200: до 3.9.8.9

Vigor 2133: до 3.9.9

Vigor 2762: до 3.9.9

Vigor 2832: до 3.9.9

Vigor 2860: до 3.9.8

Vigor 2925: до 3.9.8

Vigor 2862: до 3.9.9.5

Vigor 2926: до 3.9.9.5

Vigor 2952: до 3.9.8.2

Vigor 3220: до 3.9.8.2

Категория уязвимого продукта: Телекоммуникационное оборудование

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

**Вектор атаки:** Смежная сеть

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-03 / 2024-10-03

**Ссылки на источник:**

- <http://www.forescout.com/resources/draybreak-draytek-research/>

**Краткое описание:** Выполнение произвольного кода в Google ChromeOS LTS

**Идентификатор уязвимости:** CVE-2024-47177  
BDU:2024-07526

**Идентификатор программной ошибки:** CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

**Уязвимый продукт:** Chrome OS: до 126.0.6478.254

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

**Способ эксплуатации:** Некорректная проверка входных данных.

**Последствия эксплуатации:** Выполнение произвольного кода

58 **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:** 9.0 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-03 / 2024-10-03

**Ссылки на источник:**

- <http://chromereleases.googleblog.com/2024/10/long-term-support-lts-channel-for.html>
- <https://bdu.fstec.ru/vul/2024-07526>

**Краткое описание:** Получение конфиденциальной информации в Google ChromeOS LTS

**Идентификатор уязвимости:** CVE-2024-47175  
BDU:2024-07645

**Идентификатор программной ошибки:** CWE-20 Некорректная проверка входных данных

**Уязвимый продукт:** Chrome OS: до 126.0.6478.254

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

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** Получение конфиденциальной информации

59 **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:H/A:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-03 / 2024-10-03

**Ссылки на источник:**

- <http://chromereleases.googleblog.com/2024/10/long-term-support-lts-channel-for.html>
- <https://bdu.fstec.ru/vul/2024-07645>

**Краткое описание:** Получение конфиденциальной информации в Google ChromeOS LTS

**Идентификатор уязвимости:** CVE-2024-47076  
BDU:2024-07644

**Идентификатор программной ошибки:** CWE-20 Некорректная проверка входных данных

**Уязвимый продукт:** Chrome OS: до 126.0.6478.254

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

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** Получение конфиденциальной информации

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-03 / 2024-10-03

**Ссылки на источник:**

- <http://chromereleases.googleblog.com/2024/10/long-term-support-lts-channel-for.html>
- <https://bdu.fstec.ru/vul/2024-07644>