НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-03-02.1 | 2 марта 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2025-58360	GeoServer	Сетевой	DoS	2025-11-26	✓
2	Высокая	CVE-2026-2649	Google ChromeOS LTS	Сетевой	ACE	2026-02-28	✓
3	Высокая	CVE-2026-0902	Google ChromeOS LTS	Сетевой	OSI	2026-02-28	✓
4	Высокая	CVE-2025-37890	Google ChromeOS LTS	Локальный	PE	2026-02-28	✓
5	Высокая	CVE-2025-38000	Google ChromeOS LTS	Локальный	PE	2026-02-28	✓
6	Высокая	CVE-2026-2441	Google ChromeOS LTS	Сетевой	ACE	2026-02-28	✓
7	Высокая	CVE-2025-38350	Google ChromeOS LTS	Локальный	PE	2026-02-28	✓
8	Высокая	CVE-2025-38618	Google ChromeOS LTS	Локальный	PE	2026-02-28	✓
9	Критическая	CVE-2026-3061	Microsoft Edge	Сетевой	OSI	2026-02-27	✓
10	Критическая	CVE-2026-3062	Microsoft Edge	Сетевой	ACE	2026-02-27	✓
11	Высокая	CVE-2025-21704	Google ChromeOS	Локальный	PE	2026-02-26	✓
12	Высокая	CVE-2026-2314	Google ChromeOS	Сетевой	ACE	2026-02-26	✓
13	Высокая	CVE-2026-2313	Google ChromeOS	Сетевой	ACE	2026-02-26	✓

14	Высокая	CVE-2026-2321	Google ChromeOS	Сетевой	OSI	2026-02-26	✓
15	Высокая	CVE-2025-38349	Google ChromeOS	Локальный	PE	2026-02-26	✓
16	Высокая	CVE-2026-2319	Google ChromeOS	Сетевой	SB	2026-02-26	✓
17	Высокая	CVE-2026-2441	Google ChromeOS	Сетевой	ACE	2026-02-26	✓
18	Высокая	CVE-2026-2649	Google ChromeOS	Сетевой	ACE	2026-02-26	✓
19	Высокая	CVE-2026-2648	Google ChromeOS	Сетевой	ACE	2026-02-26	✓
20	Высокая	CVE-2026-2650	Google ChromeOS	Сетевой	ACE	2026-02-26	✓
21	Критическая	CVE-2026-21902	Juniper Networks Junos OS Evolved on PTX Series	Сетевой	ACE	2026-02-26	✓
22	Критическая	CVE-2026-20127	Cisco Catalyst SD-WAN Controller	Сетевой	SB	2026-02-25	✓
23	Высокая	CVE-2026-20128	Catalyst SD-WAN Manager	Локальный	RLF	2026-02-25	✓
24	Высокая	CVE-2026-20126	Catalyst SD-WAN Manager	Сетевой	PE	2026-02-25	✓
25	Критическая	CVE-2026-20129	Catalyst SD-WAN Manager	Сетевой	SB	2026-02-25	✓
26	Критическая	CVE-2026-2800	Mozilla Firefox и Thunderbird	Сетевой	OSI	2026-02-24	✓
27	Высокая	CVE-2026-2801	Mozilla Firefox и Thunderbird	Сетевой	DoS	2026-02-24	✓
28	Высокая	CVE-2026-2803	Mozilla Firefox и Thunderbird	Сетевой	OSI	2026-02-24	✓

29	Критическая	CVE-2026-2805	Mozilla Firefox и Thunderbird	Сетевой	DoS	2026-02-24	✓
30	Критическая	CVE-2026-2807	Mozilla Firefox и Thunderbird	Сетевой	ACE	2026-02-24	✓
31	Критическая	CVE-2026-2806	Mozilla Firefox и Thunderbird	Сетевой	OSI	2026-02-24	✓
32	Высокая	CVE-2026-2794	Mozilla Firefox	Сетевой	OSI	2026-02-24	✓
33	Критическая	CVE-2026-2795	Mozilla Firefox и Thunderbird	Сетевой	ACE	2026-02-24	✓
34	Критическая	CVE-2026-2796	Mozilla Firefox и Thunderbird	Сетевой	ACE	2026-02-24	✓
35	Критическая	CVE-2026-2797	Mozilla Firefox и Thunderbird	Сетевой	ACE	2026-02-24	✓
36	Высокая	CVE-2026-2798	Mozilla Firefox и Thunderbird	Сетевой	ACE	2026-02-24	✓
37	Критическая	CVE-2026-2799	Mozilla Firefox и Thunderbird	Сетевой	ACE	2026-02-24	✓
38	Критическая	CVE-2026-2782	Mozilla Firefox и Thunderbird ESR	Сетевой	PE	2026-02-24	✓
39	Критическая	CVE-2026-2784	Mozilla Firefox и Thunderbird ESR	Сетевой	OSI	2026-02-24	✓
40	Критическая	CVE-2026-2785	Mozilla Firefox и Thunderbird ESR	Сетевой	DoS	2026-02-24	✓
41	Высокая	CVE-2026-2783	Mozilla Firefox и Thunderbird ESR	Сетевой	OSI	2026-02-24	✓
42	Критическая	CVE-2026-2786	Mozilla Firefox и Thunderbird ESR	Сетевой	DoS	2026-02-24	✓
43	Критическая	CVE-2026-2790	Mozilla Firefox и Thunderbird ESR	Сетевой	OSI	2026-02-24	✓

44	Критическая	CVE-2026-2791	Mozilla Firefox и Thunderbird ESR	Сетевой	OSI	2026-02-24	✓
45	Критическая	CVE-2026-2765	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
46	Критическая	CVE-2026-2762	Mozilla Firefox	Сетевой	ACE	2026-02-24	✓
47	Критическая	CVE-2026-2766	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
48	Критическая	CVE-2026-2767	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
49	Критическая	CVE-2026-2768	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
50	Критическая	CVE-2026-2779	Mozilla Firefox и Thunderbird ESR	Сетевой	DoS	2026-02-24	✓
51	Критическая	CVE-2026-2780	Mozilla Firefox и Thunderbird ESR	Сетевой	PE	2026-02-24	✓
52	Критическая	CVE-2026-2781	Mozilla Firefox и Thunderbird ESR	Сетевой	DoS	2026-02-24	✓
53	Критическая	CVE-2026-2792	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
54	Критическая	CVE-2026-2793	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
55	Критическая	CVE-2026-2758	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
56	Критическая	CVE-2026-2759	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
57	Критическая	CVE-2026-2760	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
58	Критическая	CVE-2026-2761	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓

59	Критическая	CVE-2026-2763	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
60	Критическая	CVE-2026-2764	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
61	Высокая	CVE-2026-2769	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
62	Критическая	CVE-2026-2770	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
63	Критическая	CVE-2026-2771	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
64	Критическая	CVE-2026-2772	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
65	Критическая	CVE-2026-2773	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
66	Критическая	CVE-2026-2774	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
67	Критическая	CVE-2026-2775	Mozilla Firefox и Thunderbird ESR	Сетевой	SB	2026-02-24	✓
68	Критическая	CVE-2026-2757	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
69	Критическая	CVE-2026-2776	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
70	Критическая	CVE-2026-2778	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
71	Критическая	CVE-2026-2787	Mozilla Firefox и Thunderbird ESR	Сетевой	DoS	2026-02-24	✓
72	Критическая	CVE-2026-2788	Mozilla Firefox и Thunderbird ESR	Сетевой	DoS	2026-02-24	✓
73	Критическая	CVE-2026-2789	Mozilla Firefox и Thunderbird ESR	Сетевой	DoS	2026-02-24	✓

74	Критическая	CVE-2026-2777	Mozilla Firefox и Thunderbird ESR	Сетевой	ACE	2026-02-24	✓
75	Критическая	CVE-2025-13942	Zyxel products	Сетевой	ACE	2026-02-24	✓
76	Высокая	CVE-2026-22720	VMware Aria Operations	Сетевой	XSS\CSS	2026-02-24	✓
77	Высокая	CVE-2026-22719	VMware Aria Operations	Сетевой	ACE	2026-02-24	✓
78	Критическая	CVE-2026-3062	Google Chrome	Сетевой	ACE	2026-02-23	✓
79	Критическая	CVE-2026-3061	Google Chrome	Сетевой	OSI	2026-02-23	✓

1

Краткое описание: Отказ в обслуживании в GeoServer

Идентификатор уязвимости: CVE-2025-58360
2025-14710

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

Уязвимый продукт: GeoServer: до 2.26.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных 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: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-26 / 2025-11-26

Ссылки на источник:

- https://osgeo-org.atlassian.net/browse/GEOS-11682
- https://github.com/geoserver/geoserver/security/advisories/GHSA-fjf5-xgmq-5525
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv

2

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-2649

Идентификатор программной ошибки: CWE-472 Возможность изменения извне предположительно неизменяемых веб-параметров

Уязвимый продукт: Chrome OS: до 138.0.7204.305

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-28 / 2026-02-28

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/long-term-support-channel-update-for_27.html

3

Краткое описание: Получение конфиденциальной информации в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-0902

Идентификатор программной ошибки: CWE-474 Использование функции с непоследовательной реализацией

Уязвимый продукт: Chrome OS: до 138.0.7204.305

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-28 / 2026-02-28

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/long-term-support-channel-update-for_27.html

4

Краткое описание: Повышение привилегий в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2025-37890

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 138.0.7204.305

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-28 / 2026-02-28

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/long-term-support-channel-update-for_27.html

5

Краткое описание: Повышение привилегий в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2025-38000

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 138.0.7204.305

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-28 / 2026-02-28

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/long-term-support-channel-update-for_27.html

6

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-2441

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 138.0.7204.305

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-28 / 2026-02-28

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/long-term-support-channel-update-for_27.html

7

Краткое описание: Повышение привилегий в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2025-38350

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 138.0.7204.305

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-28 / 2026-02-28

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/long-term-support-channel-update-for_27.html

8

Краткое описание: Повышение привилегий в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2025-38618

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 138.0.7204.305

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-28 / 2026-02-28

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/long-term-support-channel-update-for_27.html

9

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3061

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.70

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-27 / 2026-02-27

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_23.html
- https://crbug.com/485287859
- https://crbug.com/483751167
- https://crbug.com/482862710

10

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3062

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.70

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-27 / 2026-02-27

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_23.html
- https://crbug.com/485287859
- https://crbug.com/483751167
- https://crbug.com/482862710

11

Краткое описание: Повышение привилегий в Google ChromeOS

Идентификатор уязвимости: CVE-2025-21704

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Chrome OS: до 145.0.7632.154

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Запись за пределами буфера.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-26 / 2026-02-26

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-chromeos_26.html

12

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2026-2314

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Chrome OS: до 145.0.7632.154

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-26 / 2026-02-26

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-chromeos_26.html

13

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2026-2313

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 145.0.7632.154

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-26 / 2026-02-26

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-chromeos_26.html

14

Краткое описание: Получение конфиденциальной информации в Google ChromeOS

Идентификатор уязвимости: CVE-2026-2321

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 145.0.7632.154

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-26 / 2026-02-26

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-chromeos_26.html

15

Краткое описание: Повышение привилегий в Google ChromeOS

Идентификатор уязвимости: CVE-2025-38349

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 145.0.7632.154

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-26 / 2026-02-26

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-chromeos_26.html

16

Краткое описание: Обход безопасности в Google ChromeOS

Идентификатор уязвимости: CVE-2026-2319

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

Уязвимый продукт: Chrome OS: до 145.0.7632.154

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 7.5 AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-26 / 2026-02-26

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-chromeos_26.html

17

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2026-2441

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 145.0.7632.154

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-26 / 2026-02-26

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-chromeos_26.html

18

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2026-2649

Идентификатор программной ошибки: CWE-472 Возможность изменения извне предположительно неизменяемых веб-параметров

Уязвимый продукт: Chrome OS: до 145.0.7632.154

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-26 / 2026-02-26

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-chromeos_26.html

19

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2026-2648

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

Уязвимый продукт: Chrome OS: до 145.0.7632.154

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-26 / 2026-02-26

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-chromeos_26.html

20

Краткое описание: Выполнение произвольного кода в Google ChromeOS

Идентификатор уязвимости: CVE-2026-2650

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

Уязвимый продукт: Chrome OS: до 145.0.7632.154

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-26 / 2026-02-26

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-chromeos_26.html

21

Краткое описание: Выполнение произвольного кода в Juniper Networks Junos OS Evolved on PTX Series

Идентификатор уязвимости: CVE-2026-21902

Идентификатор программной ошибки: CWE-732 Некорректные разрешения для критически важных ресурсов

Уязвимый продукт: Junos OS Evolved: 25.4R1-EVO

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

Оценка CVSSv4: 9.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:L/AU:Y/R:U/RE:M/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-26 / 2026-02-26

Ссылки на источник:

- https://supportportal.juniper.net/s/article/2026-02-Out-of-Cycle-Security-Bulletin-Junos-OS-Evolved-PTX-Series-A-vulnerability-allows-a-unauthenticated-network-based-attacker-to-execute-code-as-root-CVE-2026-21902

Краткое описание: Обход безопасности в Cisco Catalyst SD-WAN Controller

Идентификатор уязвимости: CVE-2026-20127

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Catalyst SD-WAN Controller (formerly SD-WAN vSmart): до 20.9.8.2
Catalyst SD-WAN Manager (formerly SD-WAN vManage): до 20.9.8.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Обход безопасности

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

22

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-25 / 2026-02-25

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa-EHchtZk
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCws52722

23

Краткое описание: Чтение локальных файлов в Catalyst SD-WAN Manager

Идентификатор уязвимости: CVE-2026-20128

Идентификатор программной ошибки: CWE-257 Небезопасное хранение пароля, допускающее его повторное использование

Уязвимый продукт: Catalyst SD-WAN Manager (formerly SD-WAN vManage): до 20.9.8.2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Использование жестко закодированного пароля

Последствия эксплуатации: Чтение локальных файлов

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-25 / 2026-02-25

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v
- https://bst.cisco.com/bugsearch/bug/CSCws33587
- https://bst.cisco.com/bugsearch/bug/CSCws93470
- https://bst.cisco.com/bugsearch/bug/CSCws33585
- https://bst.cisco.com/bugsearch/bug/CSCws33583
- https://bst.cisco.com/bugsearch/bug/CSCws33586
- https://bst.cisco.com/bugsearch/bug/CSCws33584

24

Краткое описание: Повышение привилегий в Catalyst SD-WAN Manager

Идентификатор уязвимости: CVE-2026-20126

Идентификатор программной ошибки: CWE-648 Некорректное использование привилегированных API

Уязвимый продукт: Catalyst SD-WAN Manager (formerly SD-WAN vManage): до 20.9.8.2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Обход процесса авторизации

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-25 / 2026-02-25

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v
- https://bst.cisco.com/bugsearch/bug/CSCws33587
- https://bst.cisco.com/bugsearch/bug/CSCws93470
- https://bst.cisco.com/bugsearch/bug/CSCws33585
- https://bst.cisco.com/bugsearch/bug/CSCws33583
- https://bst.cisco.com/bugsearch/bug/CSCws33586
- https://bst.cisco.com/bugsearch/bug/CSCws33584

25

Краткое описание: Обход безопасности в Catalyst SD-WAN Manager

Идентификатор уязвимости: CVE-2026-20129

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Catalyst SD-WAN Manager (formerly SD-WAN vManage): до 20.9.8.2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-25 / 2026-02-25

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-authbp-qwCX8D4v
- https://bst.cisco.com/bugsearch/bug/CSCws33587
- https://bst.cisco.com/bugsearch/bug/CSCws93470
- https://bst.cisco.com/bugsearch/bug/CSCws33585
- https://bst.cisco.com/bugsearch/bug/CSCws33583
- https://bst.cisco.com/bugsearch/bug/CSCws33586
- https://bst.cisco.com/bugsearch/bug/CSCws33584

26

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox и Thunderbird

Идентификатор уязвимости: CVE-2026-2800

Идентификатор программной ошибки: CWE-290 Обход аутентификации, связанный с подменой данных

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 141.0 - 147.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-16/

Краткое описание: Отказ в обслуживании в Mozilla Firefox и Thunderbird

Идентификатор уязвимости: CVE-2026-2801

Идентификатор программной ошибки: CWE-754 Некорректная проверка наличия нестандартных условий или исключений

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 141.0 - 147.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-16/

28

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox и Thunderbird

Идентификатор уязвимости: CVE-2026-2803

Идентификатор программной ошибки: CWE-200 Разглашение важной информации лицам без соответствующих прав

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 141.0 - 147.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-16/

29

Краткое описание: Отказ в обслуживании в Mozilla Firefox и Thunderbird

Идентификатор уязвимости: CVE-2026-2805

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 141.0 - 147.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-16/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird

Идентификатор уязвимости: CVE-2026-2807

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 141.0 - 147.0.2

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-16/

31

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox и Thunderbird

Идентификатор уязвимости: CVE-2026-2806

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 141.0 - 147.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-16/

32

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox

Идентификатор уязвимости: CVE-2026-2794

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/

33

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird

Идентификатор уязвимости: CVE-2026-2795

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 141.0 - 147.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-16/

34

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird

Идентификатор уязвимости: CVE-2026-2796

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 141.0 - 147.0.2

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-16/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird

Идентификатор уязвимости: CVE-2026-2797

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 141.0 - 147.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-16/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird

Идентификатор уязвимости: CVE-2026-2798

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 141.0 - 147.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-16/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird

Идентификатор уязвимости: CVE-2026-2799

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 141.0 - 147.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

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:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-16/

Краткое описание: Повышение привилегий в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2782

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2784

Идентификатор программной ошибки: CWE-288 Обход аутентификации, связанный с альтернативными путями или каналами

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Отказ в обслуживании в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2785

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

41

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2783

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Отказ в обслуживании в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2786

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Отказ в обслуживании

42

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2790

Идентификатор программной ошибки: CWE-346 Уязвимости, связанные с проверкой источника

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2791

Идентификатор программной ошибки: CWE-288 Обход аутентификации, связанный с альтернативными путями или каналами

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2765

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2026-2762

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

46

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2766

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

47 **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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2767

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

48

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2768

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

49

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Отказ в обслуживании в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2779

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Отказ в обслуживании

50

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Повышение привилегий в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2780

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Повышение привилегий

51

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Отказ в обслуживании в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2781

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Отказ в обслуживании

52

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2792

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2793

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

54

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2758

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

55

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2759

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

56 **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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2760

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

57

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2761

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2763

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2764

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

60

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2769

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

61

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2770

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

62

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

63

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2771

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2772

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

64

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2773

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

65

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

66

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2774

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Обход безопасности в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2775

Идентификатор программной ошибки: CWE-288 Обход аутентификации, связанный с альтернативными путями или каналами

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Обход безопасности

67

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2757

Идентификатор программной ошибки: Не определено

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

68

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2776

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

69

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2778

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

70

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Отказ в обслуживании в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2787

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Отказ в обслуживании

71

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Отказ в обслуживании в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2788

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

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Отказ в обслуживании

72

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Отказ в обслуживании в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2789

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Отказ в обслуживании

73

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-2777

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Mozilla Firefox: 100.0 - 147.0.4
Firefox ESR: 102.0 - 140.7.1
Firefox for Android: 100.1.0 - 147.0.4
Firefox Focus for Android: до 148.0
Mozilla Thunderbird: 102.0 - 140.7.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

74

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-25

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-14/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-15/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-13/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-17/

75

Краткое описание: Выполнение произвольного кода в Zyxel products

Идентификатор уязвимости: CVE-2025-13942

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

Уязвимый продукт: LTE3301-PLUS: до 1.00(ABQU.8)C0
NR7101: все версии
Nebula LTE3301-PLUS: до 1.18(ACCA.6)C0
Nebula NR7101: все версии
DX4510-B0: до 5.17(ABYL.10)C0
DX4510-B1: до 5.17(ABYL.10)C0
EE6510-10: до 5.19(ACJQ.4)C0
EMG6726-B10A: до 5.13(ABNP.8.1)C1
EX2210-T0: до 5.50(ACDI.2.3)C0
EX3510-B0: до 5.17(ABUP.15.1)C0
EX3510-B1: до 5.17(ABUP.15.1)C0
EX5510-B0: до 5.17(ABQX.11)C0
EX5512-T0: до 5.70(ACEG.5.3)C0
EX7710-B0: до 5.18(ACAK.1.5)C0
VMG4927-B50A: до 5.13(ABLY.10.1)C0
PX3321-T1: до 5.44(ACJB.1.4)C0,5.44(ACHK.2)C0
PX5301-T0: до 5.44(ACKB.0.5)C0
WX5610-B0: 5.18(ACGJ.0.4)C0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-24

Ссылки на источник:

- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-null-pointer-dereference-and-command-injection-vulnerabilities-in-certain-4g-lte-5g-nr-cpe-dsl-ethernet-cpe-fiber-onts-security-routers-and-wireless-extenders-02-24-2026

76

Краткое описание: Межсайтовый скриптинг в VMware Aria Operations

Идентификатор уязвимости: CVE-2026-22720

Идентификатор программной ошибки: CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев)

Уязвимый продукт: VMware Aria Operations (formerly vRealize Operations): 6.0.0 - 9.0.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Внедрение HTML-кода.

Последствия эксплуатации: Межсайтовый скриптинг

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-24

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947

77

Краткое описание: Выполнение произвольного кода в VMware Aria Operations

Идентификатор уязвимости: CVE-2026-22719

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

Уязвимый продукт: VMware Aria Operations (formerly vRealize Operations): 6.0.0 - 9.0.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-24 / 2026-02-24

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36947

78

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3062

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.110

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-23 / 2026-02-23

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_23.html
- https://crbug.com/482862710
- https://crbug.com/483751167
- https://crbug.com/485287859

79

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-3061

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.110

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-23 / 2026-02-23

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/02/stable-channel-update-for-desktop_23.html
- https://crbug.com/482862710
- https://crbug.com/483751167
- https://crbug.com/485287859