НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-05-13.1 | 13 мая 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-44420	FreeRDP	Сетевой	ACE	2026-05-12	✓
2	Высокая	CVE-2026-7363	Google ChromeOS LTS	Сетевой	ACE	2026-05-12	✓
3	Критическая	CVE-2026-5290	Google ChromeOS LTS	Сетевой	ACE	2026-05-12	✓
4	Высокая	CVE-2026-3922	Google ChromeOS LTS	Сетевой	ACE	2026-05-12	✓
5	Высокая	CVE-2026-5872	Google ChromeOS LTS	Сетевой	ACE	2026-05-12	✓
6	Высокая	CVE-2026-6303	Google ChromeOS LTS	Сетевой	ACE	2026-05-12	✓
7	Высокая	CVE-2026-5866	Google ChromeOS LTS	Сетевой	ACE	2026-05-12	✓
8	Высокая	CVE-2026-4454	Google ChromeOS LTS	Сетевой	ACE	2026-05-12	✓
9	Высокая	CVE-2026-3923	Google ChromeOS LTS	Сетевой	ACE	2026-05-12	✓
10	Высокая	CVE-2026-5280	Google ChromeOS LTS	Сетевой	ACE	2026-05-12	✓
11	Высокая	CVE-2026-3921	Google ChromeOS LTS	Сетевой	ACE	2026-05-12	✓
12	Высокая	CVE-2026-8093	Mozilla Thunderbird	Сетевой	ACE	2026-05-11	✓
13	Высокая	CVE-2026-8092	Mozilla Thunderbird и Thunderbird ESR	Сетевой	ACE	2026-05-11	✓

14	Критическая	CVE-2026-8094	Mozilla Thunderbird ESR	Сетевой	ACE	2026-05-11	✓
15	Высокая	CVE-2026-7258	PHP	Сетевой	DoS	2026-05-10	✓
16	Высокая	CVE-2026-7568	PHP	Сетевой	DoS	2026-05-10	✓
17	Высокая	CVE-2026-7262	PHP	Сетевой	DoS	2026-05-10	✓
18	Критическая	CVE-2026-7261	PHP	Сетевой	DoS	2026-05-10	✓
19	Критическая	CVE-2026-6722	PHP	Сетевой	DoS	2026-05-10	✓
20	Критическая	CVE-2025-14179	PHP	Сетевой	ACE	2026-05-10	✓
21	Критическая	CVE-2026-6104	PHP	Сетевой	DoS	2026-05-10	✓
22	Высокая	CVE-2026-7263	PHP	Сетевой	OSI	2026-05-10	✓
23	Высокая	CVE-2026-7930	Google Chrome	Сетевой	OSI	2026-05-07	✓
24	Высокая	CVE-2026-7938	Google Chrome	Сетевой	OSI	2026-05-07	✓
25	Высокая	CVE-2026-7940	Google Chrome	Сетевой	OSI	2026-05-07	✓
26	Высокая	CVE-2026-7929	Google Chrome	Сетевой	ACE	2026-05-07	✓
27	Высокая	CVE-2026-7948	Google Chrome	Сетевой	SB	2026-05-07	✓
28	Высокая	CVE-2026-7951	Google Chrome	Сетевой	ACE	2026-05-07	✓

29	Высокая	CVE-2026-7956	Google Chrome	Сетевой	OSI	2026-05-07	✓
30	Высокая	CVE-2026-7957	Google Chrome	Сетевой	ACE	2026-05-07	✓
31	Высокая	CVE-2026-7928	Google Chrome	Сетевой	ACE	2026-05-07	✓
32	Высокая	CVE-2026-7926	Google Chrome	Сетевой	ACE	2026-05-07	✓
33	Высокая	CVE-2026-7897	Google Chrome	Сетевой	ACE	2026-05-07	✓
34	Высокая	CVE-2026-7898	Google Chrome	Сетевой	ACE	2026-05-07	✓
35	Высокая	CVE-2026-7899	Google Chrome	Сетевой	ACE	2026-05-07	✓
36	Высокая	CVE-2026-7900	Google Chrome	Сетевой	ACE	2026-05-07	✓
37	Высокая	CVE-2026-7901	Google Chrome	Сетевой	ACE	2026-05-07	✓
38	Высокая	CVE-2026-7902	Google Chrome	Сетевой	ACE	2026-05-07	✓
39	Высокая	CVE-2026-7903	Google Chrome	Сетевой	ACE	2026-05-07	✓
40	Высокая	CVE-2026-7905	Google Chrome	Сетевой	ACE	2026-05-07	✓
41	Высокая	CVE-2026-7906	Google Chrome	Сетевой	ACE	2026-05-07	✓
42	Высокая	CVE-2026-7907	Google Chrome	Сетевой	ACE	2026-05-07	✓
43	Критическая	CVE-2026-7908	Google Chrome	Сетевой	ACE	2026-05-07	✓

44	Критическая	CVE-2026-7910	Google Chrome	Сетевой	ACE	2026-05-07	✓
45	Высокая	CVE-2026-7927	Google Chrome	Сетевой	ACE	2026-05-07	✓
46	Высокая	CVE-2026-7911	Google Chrome	Сетевой	ACE	2026-05-07	✓
47	Высокая	CVE-2026-7913	Google Chrome	Локальный	SB	2026-05-07	✓
48	Высокая	CVE-2026-7914	Google Chrome	Сетевой	ACE	2026-05-07	✓
49	Высокая	CVE-2026-7916	Google Chrome	Сетевой	ACE	2026-05-07	✓
50	Высокая	CVE-2026-7917	Google Chrome	Сетевой	ACE	2026-05-07	✓
51	Высокая	CVE-2026-7918	Google Chrome	Сетевой	ACE	2026-05-07	✓
52	Высокая	CVE-2026-7919	Google Chrome	Сетевой	ACE	2026-05-07	✓
53	Высокая	CVE-2026-7920	Google Chrome	Сетевой	ACE	2026-05-07	✓
54	Высокая	CVE-2026-7921	Google Chrome	Сетевой	ACE	2026-05-07	✓
55	Высокая	CVE-2026-7922	Google Chrome	Сетевой	ACE	2026-05-07	✓
56	Высокая	CVE-2026-7923	Google Chrome	Сетевой	ACE	2026-05-07	✓
57	Высокая	CVE-2026-7925	Google Chrome	Локальный	ACE	2026-05-07	✓
58	Высокая	CVE-2026-7896	Google Chrome	Сетевой	ACE	2026-05-07	✓

59	Высокая	CVE-2026-7963	Google Chrome	Сетевой	OSI	2026-05-07	✓
60	Высокая	CVE-2026-7997	Google Chrome	Локальный	DoS	2026-05-07	✓
61	Высокая	CVE-2026-8000	Google Chrome	Сетевой	DoS	2026-05-07	✓
62	Высокая	CVE-2026-8001	Google Chrome	Сетевой	DoS	2026-05-07	✓
63	Высокая	CVE-2026-8002	Google Chrome	Сетевой	DoS	2026-05-07	✓
64	Высокая	CVE-2026-8007	Google Chrome	Сетевой	DoS	2026-05-07	✓
65	Высокая	CVE-2026-8016	Google Chrome	Сетевой	DoS	2026-05-07	✓
66	Высокая	CVE-2026-8018	Google Chrome	Сетевой	OSI	2026-05-07	✓
67	Высокая	CVE-2026-7995	Google Chrome	Сетевой	OSI	2026-05-07	✓
68	Высокая	CVE-2026-7967	Google Chrome	Сетевой	OSI	2026-05-07	✓
69	Высокая	CVE-2026-7970	Google Chrome	Сетевой	OSI	2026-05-07	✓
70	Высокая	CVE-2026-7973	Google Chrome	Сетевой	DoS	2026-05-07	✓
71	Высокая	CVE-2026-7974	Google Chrome	Сетевой	OSI	2026-05-07	✓
72	Высокая	CVE-2026-7975	Google Chrome	Сетевой	OSI	2026-05-07	✓
73	Высокая	CVE-2026-7976	Google Chrome	Сетевой	OSI	2026-05-07	✓

74	Высокая	CVE-2026-7994	Google Chrome	Локальный	OSI	2026-05-07	✓
75	Высокая	CVE-2026-7978	Google Chrome	Сетевой	OSI	2026-05-07	✓
76	Высокая	CVE-2026-7980	Google Chrome	Сетевой	OSI	2026-05-07	✓
77	Высокая	CVE-2026-7981	Google Chrome	Сетевой	OSI	2026-05-07	✓
78	Высокая	CVE-2026-7984	Google Chrome	Сетевой	OSI	2026-05-07	✓
79	Высокая	CVE-2026-7985	Google Chrome	Сетевой	OSI	2026-05-07	✓
80	Высокая	CVE-2026-7987	Google Chrome	Сетевой	OSI	2026-05-07	✓
81	Высокая	CVE-2026-7988	Google Chrome	Сетевой	OSI	2026-05-07	✓
82	Высокая	CVE-2026-7990	Google Chrome	Локальный	OSI	2026-05-07	✓
83	Высокая	CVE-2026-7991	Google Chrome	Сетевой	OSI	2026-05-07	✓
84	Высокая	CVE-2026-7992	Google Chrome	Сетевой	OSI	2026-05-07	✓
85	Высокая	CVE-2025-9086	Juniper Secure Analytics	Сетевой	DoS	2026-05-06	✓
86	Высокая	CVE-2025-38129	Juniper Secure Analytics	Локальный	PE	2026-05-06	✓
87	Высокая	CVE-2025-38248	Juniper Secure Analytics	Локальный	PE	2026-05-06	✓
88	Высокая	CVE-2026-23001	Juniper Secure Analytics	Локальный	PE	2026-05-06	✓

89	Высокая	CVE-2026-23074	Juniper Secure Analytics	Локальный	PE	2026-05-06	✓
90	Критическая	CVE-2026-0300	User-ID Authentication Portal on Palo Alto PAN-OS	Сетевой	ACE	2026-05-06	✗
91	Критическая	CVE-2026-24118	vm2	Сетевой	ACE	2026-05-04	✓
92	Критическая	CVE-2026-24781	vm2	Сетевой	ACE	2026-05-04	✓
93	Критическая	CVE-2026-26332	vm2	Сетевой	ACE	2026-05-04	✓
94	Критическая	CVE-2026-24120	vm2	Сетевой	ACE	2026-05-04	✓
95	Критическая	CVE-2026-26956	vm2	Сетевой	ACE	2026-05-04	✓
96	Высокая	CVE-2026-23918	Apache HTTP Server	Сетевой	ACE	2026-05-04	✓
97	Высокая	CVE-2026-24072	Apache HTTP Server	Сетевой	OSI	2026-05-04	✓
98	Критическая	CVE-2026-28780	Apache HTTP Server	Сетевой	ACE	2026-05-04	✓
99	Высокая	CVE-2026-29169	Apache HTTP Server	Сетевой	DoS	2026-05-04	✓
100	Высокая	CVE-2026-34059	Apache HTTP Server	Сетевой	OSI	2026-05-04	✓

1

Краткое описание: Выполнение произвольного кода в FreeRDP

Идентификатор уязвимости: CVE-2026-44420

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

Уязвимый продукт: FreeRDP: 3.0.0 - 3.25.0

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: 8.8 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: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-j9q5-7g8m-jc9v
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-mpxh-8fq3-x8mh
- https://github.com/FreeRDP/FreeRDP/commit/a0be5cb87d760bb1c803ad1bb835aa1e73e62abc
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-p6r2-4hgm-m6ff
- https://github.com/FreeRDP/FreeRDP/commit/23b36cd00ebf0ccd97750fcdbc9aa2f362352da7
- https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-mvpx-xj7r-3p3r

2

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-7363

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 144.0.7559.250

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/long-term-support-channel-update-for.html

3	**Краткое описание:** Выполнение произвольного кода в Google ChromeOS LTS **Идентификатор уязвимости:** CVE-2026-5290 **Идентификатор программной ошибки:** CWE-416 Использование после освобождения **Уязвимый продукт:** Chrome OS: до 144.0.7559.250 **Категория уязвимого продукта:** Unix-подобные операционные системы 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:** 9.6 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H **Оценка CVSSv4:** Не определено **Вектор атаки:** Сетевой **Взаимодействие с пользователем:** Требуется **Дата выявления / Дата обновления:** 2026-05-12 / 2026-05-12 **Ссылки на источник:** • https://chromereleases.googleblog.com/2026/05/long-term-support-channel-update-for.html

4

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-3922

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 144.0.7559.250

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/long-term-support-channel-update-for.html

5

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-5872

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 144.0.7559.250

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/long-term-support-channel-update-for.html

6

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-6303

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 144.0.7559.250

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/long-term-support-channel-update-for.html

7

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-5866

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 144.0.7559.250

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/long-term-support-channel-update-for.html

8

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-4454

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 144.0.7559.250

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/long-term-support-channel-update-for.html

9

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-3923

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 144.0.7559.250

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/long-term-support-channel-update-for.html

10

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-5280

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 144.0.7559.250

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/long-term-support-channel-update-for.html

11

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-3921

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 144.0.7559.250

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

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/long-term-support-channel-update-for.html

12

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2026-8093

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

Уязвимый продукт: Mozilla Thunderbird: 150.0 - 150.0.1

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: 2026-05-11 / 2026-05-11

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-43/

13

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

Идентификатор уязвимости: CVE-2026-8092

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Mozilla Thunderbird: 102.0 - 140.9.1
Mozilla Thunderbird: 150.0 - 150.0.1

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: 2026-05-11 / 2026-05-11

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-43/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-44/

14

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird ESR

Идентификатор уязвимости: CVE-2026-8094

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: Mozilla Thunderbird: 102.0 - 140.9.1

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: 2026-05-11 / 2026-05-11

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-44/

15

Краткое описание: Отказ в обслуживании в PHP

Идентификатор уязвимости: CVE-2026-7258

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PHP: 8.0.0 - 8.5.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 6.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:L/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-10 / 2026-05-10

Ссылки на источник:

- https://www.php.net/ChangeLog-8.php#8.5.6
- https://www.php.net/ChangeLog-8.php#8.4.21

16

Краткое описание: Отказ в обслуживании в PHP

Идентификатор уязвимости: CVE-2026-7568

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PHP: 8.0.0 - 8.5.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 6.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L/RE:L/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-10 / 2026-05-10

Ссылки на источник:

- https://www.php.net/ChangeLog-8.php#8.5.6
- https://www.php.net/ChangeLog-8.php#8.4.21

17

Краткое описание: Отказ в обслуживании в PHP

Идентификатор уязвимости: CVE-2026-7262

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: PHP: 8.0.0 - 8.5.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 2.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:P/AU:Y/RE:M/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-10 / 2026-05-10

Ссылки на источник:

- https://www.php.net/ChangeLog-8.php#8.5.6
- https://www.php.net/ChangeLog-8.php#8.4.21

18

Краткое описание: Отказ в обслуживании в PHP

Идентификатор уязвимости: CVE-2026-7261

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: PHP: 8.0.0 - 8.5.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированного запроса.

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: 6.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:L/SC:L/SI:L/SA:L/S:P/AU:Y/RE:M/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-10 / 2026-05-10

Ссылки на источник:

- https://www.php.net/ChangeLog-8.php#8.5.6
- https://www.php.net/ChangeLog-8.php#8.4.21

19

Краткое описание: Отказ в обслуживании в PHP

Идентификатор уязвимости: CVE-2026-6722

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: PHP: 8.0.0 - 8.5.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированного запроса.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-10 / 2026-05-10

Ссылки на источник:

- https://www.php.net/ChangeLog-8.php#8.5.6
- https://www.php.net/ChangeLog-8.php#8.4.21

20

Краткое описание: Выполнение произвольного кода в PHP

Идентификатор уязвимости: CVE-2025-14179

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

Уязвимый продукт: PHP: 8.0.0 - 8.5.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.0 AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/E:P/AU:Y/RE:M/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-10 / 2026-05-10

Ссылки на источник:

- https://www.php.net/ChangeLog-8.php#8.5.6
- https://www.php.net/ChangeLog-8.php#8.4.21

21

Краткое описание: Отказ в обслуживании в PHP

Идентификатор уязвимости: CVE-2026-6104

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: PHP: 8.0.0 - 8.5.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 6.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:L/SC:L/SI:N/SA:L/RE:M/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-10 / 2026-05-10

Ссылки на источник:

- https://www.php.net/ChangeLog-8.php#8.5.6
- https://www.php.net/ChangeLog-8.php#8.4.21

22

Краткое описание: Получение конфиденциальной информации в PHP

Идентификатор уязвимости: CVE-2026-7263

Идентификатор программной ошибки: CWE-404 Некорректное освобождение ресурсов

Уязвимый продукт: PHP: 8.0.0 - 8.5.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Оценка CVSSv4: 6.0 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:L/AU:Y/RE:M/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-10 / 2026-05-10

Ссылки на источник:

- https://www.php.net/ChangeLog-8.php#8.5.6
- https://www.php.net/ChangeLog-8.php#8.4.21

23

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7930

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

24

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7938

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

25

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7940

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

26

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7929

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

27

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-7948

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368

- https://crbug.com/497975608
- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430

- https://crbug.com/496626029
- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912

- https://crbug.com/502830119
- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187

- https://crbug.com/504660052
- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

28

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7951

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

29

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7956

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

30

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7957

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

31

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7928

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

32

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7926

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

33

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7897

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

34

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7898

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

35

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7899

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

36

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7900

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

37

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7901

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

38

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7902

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

39

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7903

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

40

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7905

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

41

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7906

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

42

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7907

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

43

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7908

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

44

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7910

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

45

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7927

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

46

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7911

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

47

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-7913

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

48

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7914

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

49

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7916

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

50

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7917

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

51

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7918

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

52

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7919

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

53

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7920

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

54

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7921

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

55

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7922

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

56

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7923

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

57

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7925

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

58

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7896

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

59

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7963

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

60

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-7997

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

61

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-8000

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.8 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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

62

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-8001

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

63

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-8002

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

64

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-8007

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

65

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-8016

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

66

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-8018

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.1 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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

67

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7995

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

68

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7967

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

69

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7970

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-7973

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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

Оценка CVSSv4: Не определено

70

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

71

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7974

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

72

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7975

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

73

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7976

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

74

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7994

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7978

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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

Оценка CVSSv4: Не определено

75

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7980

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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

76

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

77

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7981

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

78

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7984

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

79

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7985

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

80

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7987

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

81

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7988

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

82

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7990

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

83

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7991

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

84

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7992

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 148.0.7778.56

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: 2026-05-07 / 2026-05-07

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop.html
- https://crbug.com/497849876
- https://crbug.com/499067529
- https://crbug.com/499065126
- https://crbug.com/498892267
- https://crbug.com/498765082
- https://crbug.com/498753456
- https://crbug.com/498696266
- https://crbug.com/498396238
- https://crbug.com/498352423
- https://crbug.com/498277368
- https://crbug.com/497975608

- https://crbug.com/497952533
- https://crbug.com/497926602
- https://crbug.com/497859275
- https://crbug.com/497828892
- https://crbug.com/499116954
- https://crbug.com/497821223
- https://crbug.com/497736679
- https://crbug.com/497735587
- https://crbug.com/497649372
- https://crbug.com/497565944
- https://crbug.com/497546281
- https://crbug.com/497529290
- https://crbug.com/497487462
- https://crbug.com/497450574
- https://crbug.com/497432281
- https://crbug.com/497365545
- https://crbug.com/497341787
- https://crbug.com/497255035
- https://crbug.com/497254383
- https://crbug.com/499099003
- https://crbug.com/501745798
- https://crbug.com/497081987
- https://crbug.com/496628298
- https://crbug.com/499194407
- https://crbug.com/498417031
- https://crbug.com/498382925
- https://crbug.com/498353173
- https://crbug.com/498292657
- https://crbug.com/497722578
- https://crbug.com/497695401
- https://crbug.com/497548558
- https://crbug.com/497490364
- https://crbug.com/497427430
- https://crbug.com/496626029

- https://crbug.com/484547631
- https://crbug.com/496624084
- https://crbug.com/496555077
- https://crbug.com/496426191
- https://crbug.com/496399759
- https://crbug.com/496373088
- https://crbug.com/496298665
- https://crbug.com/496189510
- https://crbug.com/495985532
- https://crbug.com/495779613
- https://crbug.com/494764371
- https://crbug.com/494464734
- https://crbug.com/493099941
- https://crbug.com/491676472
- https://crbug.com/487960705
- https://crbug.com/497250399
- https://crbug.com/497008295
- https://crbug.com/493747582
- https://crbug.com/497639714
- https://crbug.com/501833981
- https://crbug.com/500087204
- https://crbug.com/500080194
- https://crbug.com/499449324
- https://crbug.com/499062376
- https://crbug.com/498989348
- https://crbug.com/498832921
- https://crbug.com/498780188
- https://crbug.com/498752242
- https://crbug.com/498720754
- https://crbug.com/498454478
- https://crbug.com/498401609
- https://crbug.com/497936728
- https://crbug.com/497548912
- https://crbug.com/502830119

- https://crbug.com/497543810
- https://crbug.com/497437113
- https://crbug.com/497436531
- https://crbug.com/496292089
- https://crbug.com/496284584
- https://crbug.com/495259842
- https://crbug.com/492350406
- https://crbug.com/491760376
- https://crbug.com/502030575
- https://crbug.com/497724490
- https://crbug.com/496503799
- https://crbug.com/505481948
- https://crbug.com/504587882
- https://crbug.com/504069514
- https://crbug.com/502249087
- https://crbug.com/504612429
- https://crbug.com/497007825
- https://crbug.com/495802788
- https://crbug.com/496645205
- https://crbug.com/496632973
- https://crbug.com/496607380
- https://crbug.com/496463315
- https://crbug.com/496441232
- https://crbug.com/496380960
- https://crbug.com/496379792
- https://crbug.com/496279876
- https://crbug.com/496266456
- https://crbug.com/496259890
- https://crbug.com/496206134
- https://crbug.com/496193452
- https://crbug.com/496169594
- https://crbug.com/496016840
- https://crbug.com/495783187
- https://crbug.com/504660052

- https://crbug.com/495373657
- https://crbug.com/495363705
- https://crbug.com/493955234
- https://crbug.com/493631402
- https://crbug.com/492963096
- https://crbug.com/492735384
- https://crbug.com/491766258
- https://crbug.com/490485402
- https://crbug.com/489624550
- https://crbug.com/489023922
- https://crbug.com/488585490
- https://crbug.com/481634116
- https://crbug.com/474338157
- https://crbug.com/434825208

85

Краткое описание: Отказ в обслуживании в Juniper Secure Analytics

Идентификатор уязвимости: CVE-2025-9086

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP15

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Чтение за пределами буфера.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP15-IF01

86

Краткое описание: Повышение привилегий в Juniper Secure Analytics

Идентификатор уязвимости: CVE-2025-38129

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP15

Категория уязвимого продукта: Средства защиты информации

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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP15-IF01

87

Краткое описание: Повышение привилегий в Juniper Secure Analytics

Идентификатор уязвимости: CVE-2025-38248

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP15

Категория уязвимого продукта: Средства защиты информации

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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP15-IF01

88

Краткое описание: Повышение привилегий в Juniper Secure Analytics

Идентификатор уязвимости: CVE-2026-23001

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP15

Категория уязвимого продукта: Средства защиты информации

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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP15-IF01

89

Краткое описание: Повышение привилегий в Juniper Secure Analytics

Идентификатор уязвимости: CVE-2026-23074

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Juniper Secure Analytics (JSA): 7.5.0 - 7.5.0 UP15

Категория уязвимого продукта: Средства защиты информации

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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://supportportal.juniper.net/s/article/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-Juniper-Secure-Analytics-in-7-5-0-UP15-IF01

90

Краткое описание: Выполнение произвольного кода в User-ID Authentication Portal on Palo Alto PAN-OS

Идентификатор уязвимости: CVE-2026-0300

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Palo Alto PAN-OS: 10.2 - 12.1.4-h4

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.8 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:L/SI:L/SA:N/E:A/AU:Y/R:U/V:C/RE:M/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://security.paloaltonetworks.com/CVE-2026-0300

91

Краткое описание: Выполнение произвольного кода в vm2

Идентификатор уязвимости: CVE-2026-24118

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: vm2: 3.9.0 - 3.10.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка 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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/patriksimek/vm2/security/advisories/GHSA-55hx-c926-fr95
- https://github.com/patriksimek/vm2/security/advisories/GHSA-v37h-5mfm-c47c
- https://github.com/patriksimek/vm2/security/advisories/GHSA-grj5-jjm8-h35p
- https://github.com/patriksimek/vm2/commit/4b009c2d4b1131c01810c1205e641d614c322a29

92

Краткое описание: Выполнение произвольного кода в vm2

Идентификатор уязвимости: CVE-2026-24781

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: vm2: 3.9.0 - 3.10.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка 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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/patriksimek/vm2/security/advisories/GHSA-55hx-c926-fr95
- https://github.com/patriksimek/vm2/security/advisories/GHSA-v37h-5mfm-c47c
- https://github.com/patriksimek/vm2/security/advisories/GHSA-grj5-jjm8-h35p
- https://github.com/patriksimek/vm2/commit/4b009c2d4b1131c01810c1205e641d614c322a29

93

Краткое описание: Выполнение произвольного кода в vm2

Идентификатор уязвимости: CVE-2026-26332

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: vm2: 3.9.0 - 3.10.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка 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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/patriksimek/vm2/security/advisories/GHSA-55hx-c926-fr95
- https://github.com/patriksimek/vm2/security/advisories/GHSA-v37h-5mfm-c47c
- https://github.com/patriksimek/vm2/security/advisories/GHSA-grj5-jjm8-h35p
- https://github.com/patriksimek/vm2/commit/4b009c2d4b1131c01810c1205e641d614c322a29

94

Краткое описание: Выполнение произвольного кода в vm2

Идентификатор уязвимости: CVE-2026-24120

Идентификатор программной ошибки: CWE-94 Некорректное управление генерированием кода (внедрение кода)

Уязвимый продукт: vm2: 3.9.0 - 3.10.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка 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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/patriksimek/vm2/security/advisories/GHSA-ffh4-j6h5-pg66
- https://github.com/patriksimek/vm2/security/advisories/GHSA-qvjj-29qf-hp7p
- https://github.com/patriksimek/vm2/blob/4b009c2d4b1131c01810c1205e641d614c322a29/lib/setup-sandbox.js#L35C7-L39

95

Краткое описание: Выполнение произвольного кода в vm2

Идентификатор уязвимости: CVE-2026-26956

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: vm2: 3.9.0 - 3.10.3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка 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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://github.com/patriksimek/vm2/security/advisories/GHSA-ffh4-j6h5-pg66
- https://github.com/patriksimek/vm2/security/advisories/GHSA-qvjj-29qf-hp7p
- https://github.com/patriksimek/vm2/blob/4b009c2d4b1131c01810c1205e641d614c322a29/lib/setup-sandbox.js#L35C7-L39

96

Краткое описание: Выполнение произвольного кода в Apache HTTP Server

Идентификатор уязвимости: CVE-2026-23918

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Apache HTTP Server: 2.4 - 2.4.66

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-34059
- https://lists.apache.org/thread/2m26t0c1zhrz0wxpxdx6t1g999415yk7
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-34032
- https://lists.apache.org/thread/7dnmy4cxb8qfdgr8bs9jrn0vr0pylwkd
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33857
- https://lists.apache.org/thread/k97f307d4xgsxthgf5fzf03m9qdkvgzy
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33523
- https://lists.apache.org/thread/88f06q3opz3snbsfbyj4x6zqrzkklto6
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33007
- https://lists.apache.org/thread/4qokdcgl8q6tl3b594v72sr52g7wrbd4
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33006
- https://lists.apache.org/thread/ro2mhvozhdp1j5d8w68nwgyzr9fy2s7y

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-29169
- https://lists.apache.org/thread/0wlowdb6ydgdtxspx8og5x72bgdzgfx1
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-29168
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-28780
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-24072
- https://lists.apache.org/thread/5tg6pwqr0z9hh0v8x9h0ywgs1z3x26l2
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-23918
- https://lists.apache.org/thread/otwt07gfnp6x2b58hnbghgs9r4ovy3yf

97

Краткое описание: Получение конфиденциальной информации в Apache HTTP Server

Идентификатор уязвимости: CVE-2026-24072

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Apache HTTP Server: 2.4 - 2.4.66

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-34059
- https://lists.apache.org/thread/2m26t0c1zhrz0wxpxdx6t1g999415yk7
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-34032
- https://lists.apache.org/thread/7dnmy4cxb8qfdgr8bs9jrn0vr0pylwkd
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33857
- https://lists.apache.org/thread/k97f307d4xgsxthgf5fzf03m9qdkvgzy
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33523
- https://lists.apache.org/thread/88f06q3opz3snbsfbyj4x6zqrzkklto6
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33007
- https://lists.apache.org/thread/4qokdcgl8q6tl3b594v72sr52g7wrbd4
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33006
- https://lists.apache.org/thread/ro2mhvozhdp1j5d8w68nwgyzr9fy2s7y

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-29169
- https://lists.apache.org/thread/0wlowdb6ydgdtxspx8og5x72bgdzgfx1
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-29168
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-28780
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-24072
- https://lists.apache.org/thread/5tg6pwqr0z9hh0v8x9h0ywgs1z3x26l2
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-23918
- https://lists.apache.org/thread/otwt07gfnp6x2b58hnbghgs9r4ovy3yf

98

Краткое описание: Выполнение произвольного кода в Apache HTTP Server

Идентификатор уязвимости: CVE-2026-28780

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

Уязвимый продукт: Apache HTTP Server: 2.4 - 2.4.66

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-34059
- https://lists.apache.org/thread/2m26t0c1zhrz0wxpxdx6t1g999415yk7
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-34032
- https://lists.apache.org/thread/7dnmy4cxb8qfdgr8bs9jrn0vr0pylwkd
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33857
- https://lists.apache.org/thread/k97f307d4xgsxthgf5fzf03m9qdkvgzy
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33523
- https://lists.apache.org/thread/88f06q3opz3snbsfbyj4x6zqrzkklto6
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33007
- https://lists.apache.org/thread/4qokdcgl8q6tl3b594v72sr52g7wrbd4
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33006
- https://lists.apache.org/thread/ro2mhvozhdp1j5d8w68nwgyzr9fy2s7y

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-29169
- https://lists.apache.org/thread/0wlowdb6ydgdtxspx8og5x72bgdzgfx1
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-29168
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-28780
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-24072
- https://lists.apache.org/thread/5tg6pwqr0z9hh0v8x9h0ywgs1z3x26l2
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-23918
- https://lists.apache.org/thread/otwt07gfnp6x2b58hnbghgs9r4ovy3yf

99

Краткое описание: Отказ в обслуживании в Apache HTTP Server

Идентификатор уязвимости: CVE-2026-29169

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Apache HTTP Server: 2.4 - 2.4.66

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-34059
- https://lists.apache.org/thread/2m26t0c1zhrz0wxpxdx6t1g999415yk7
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-34032
- https://lists.apache.org/thread/7dnmy4cxb8qfdgr8bs9jrn0vr0pylwkd
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33857
- https://lists.apache.org/thread/k97f307d4xgsxthgf5fzf03m9qdkvgzy
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33523
- https://lists.apache.org/thread/88f06q3opz3snbsfbyj4x6zqrzkklto6
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33007
- https://lists.apache.org/thread/4qokdcgl8q6tl3b594v72sr52g7wrbd4
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33006
- https://lists.apache.org/thread/ro2mhvozhdp1j5d8w68nwgyzr9fy2s7y

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-29169
- https://lists.apache.org/thread/0wlowdb6ydgdtxspx8og5x72bgdzgfx1
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-29168
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-28780
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-24072
- https://lists.apache.org/thread/5tg6pwqr0z9hh0v8x9h0ywgs1z3x26l2
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-23918
- https://lists.apache.org/thread/otwt07gfnp6x2b58hnbghgs9r4ovy3yf

100

Краткое описание: Получение конфиденциальной информации в Apache HTTP Server

Идентификатор уязвимости: CVE-2026-34059

Идентификатор программной ошибки: CWE-126 Чтение за границей буфера

Уязвимый продукт: Apache HTTP Server: 2.4 - 2.4.66

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подключение к вредоносному серверу.

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: 2026-05-04 / 2026-05-04

Ссылки на источник:

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-34059
- https://lists.apache.org/thread/2m26t0c1zhrz0wxpxdx6t1g999415yk7
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-34032
- https://lists.apache.org/thread/7dnmy4cxb8qfdgr8bs9jrn0vr0pylwkd
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33857
- https://lists.apache.org/thread/k97f307d4xgsxthgf5fzf03m9qdkvgzy
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33523
- https://lists.apache.org/thread/88f06q3opz3snbsfbyj4x6zqrzkklto6
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33007
- https://lists.apache.org/thread/4qokdcgl8q6tl3b594v72sr52g7wrbd4
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-33006
- https://lists.apache.org/thread/ro2mhvozhdp1j5d8w68nwgyzr9fy2s7y

- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-29169
- https://lists.apache.org/thread/0wlowdb6ydgdtxspx8og5x72bgdzgfx1
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-29168
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-28780
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-24072
- https://lists.apache.org/thread/5tg6pwqr0z9hh0v8x9h0ywgs1z3x26l2
- https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2026-23918
- https://lists.apache.org/thread/otwt07gfnp6x2b58hnbghgs9r4ovy3yf