НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-05-06.1 | 6 мая 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	BDU:2026-04237	Cisco IOS XE	Сетевой	DoS	2026-03-30	✓
2	Высокая	BDU:2026-04594	Cisco Evolved Programmable Network Manager	Сетевой	ACE	2026-04-02	✓
3	Критическая	BDU:2026-04638	FortiClientEMS	Сетевой	ACE	2026-04-06	✓
4	Критическая	BDU:2026-05532	Cisco Webex Centers	Сетевой	ACE	2026-04-16	✓
5	Критическая	BDU:2026-04595	Cisco Smart Software Manager On-Prem	Сетевой	ACE	2026-04-02	✓
6	Критическая	BDU:2026-05531	Cisco Identity Services Engine	Сетевой	ACE	2026-04-17	✓
7	Высокая	CVE-2026-23918	Apache HTTP Server	Сетевой	ACE	2026-05-04	✓
8	Высокая	CVE-2026-29169	Apache HTTP Server	Сетевой	DoS	2026-05-04	✓
9	Высокая	CVE-2026-34059	Apache HTTP Server	Сетевой	OSI	2026-05-04	✓
10	Высокая	CVE-2026-33845	GnuTLS	Сетевой	ACE	2026-04-30	✓
11	Высокая	CVE-2026-33846	GnuTLS	Сетевой	OAF	2026-04-30	✓
12	Высокая	CVE-2026-5402	Wireshark	Сетевой	ACE	2026-04-30	✓
13	Высокая	CVE-2026-5403	Wireshark	Локальный	DoS	2026-04-30	✓

14	Высокая	CVE-2026-5405	Wireshark	Локальный	DoS	2026-04-30	✓
15	Высокая	CVE-2026-4675	Google ChromeOS LTS	Сетевой	ACE	2026-04-30	✓
16	Высокая	CVE-2026-4680	Google ChromeOS LTS	Сетевой	ACE	2026-04-30	✓
17	Высокая	CVE-2026-4456	Google ChromeOS LTS	Сетевой	ACE	2026-04-30	✓
18	Высокая	CVE-2026-6297	Google ChromeOS LTS	Сетевой	ACE	2026-04-30	✓
19	Высокая	CVE-2026-42511	FreeBSD	Сетевой	ACE	2026-04-30	✓
20	Высокая	CVE-2026-7270	FreeBSD	Локальный	PE	2026-04-30	✓
21	Высокая	CVE-2026-7164	FreeBSD	Сетевой	DoS	2026-04-30	✓
22	Высокая	CVE-2026-42512	FreeBSD	Сетевой	ACE	2026-04-30	✓
23	Высокая	CVE-2026-39457	FreeBSD	Локальный	PE	2026-04-30	✓
24	Высокая	CVE-2026-35547	FreeBSD	Сетевой	PE	2026-04-30	✓
25	Высокая	CVE-2026-0204	SonicOS	Смежная сеть	OSI	2026-04-29	✓
26	Высокая	CVE-2026-7352	Google Chrome	Сетевой	ACE	2026-04-29	✓
27	Высокая	CVE-2026-7353	Google Chrome	Сетевой	ACE	2026-04-29	✓
28	Высокая	CVE-2026-7354	Google Chrome	Сетевой	OSI	2026-04-29	✓

29	Высокая	CVE-2026-7356	Google Chrome	Сетевой	ACE	2026-04-29	✓
30	Высокая	CVE-2026-7357	Google Chrome	Сетевой	ACE	2026-04-29	✓
31	Высокая	CVE-2026-7350	Google Chrome	Сетевой	ACE	2026-04-29	✓
32	Высокая	CVE-2026-7334	Google Chrome	Сетевой	ACE	2026-04-29	✓
33	Высокая	CVE-2026-7359	Google Chrome	Сетевой	ACE	2026-04-29	✓
34	Критическая	CVE-2026-7333	Google Chrome	Сетевой	ACE	2026-04-29	✓
35	Высокая	CVE-2026-7343	Google Chrome	Сетевой	ACE	2026-04-29	✓
36	Высокая	CVE-2026-7344	Google Chrome	Сетевой	ACE	2026-04-29	✓
37	Высокая	CVE-2026-7361	Google Chrome	Сетевой	ACE	2026-04-29	✓
38	Высокая	CVE-2026-7358	Google Chrome	Сетевой	ACE	2026-04-29	✓
39	Высокая	CVE-2026-7363	Google Chrome	Сетевой	ACE	2026-04-29	✓
40	Высокая	CVE-2026-7349	Google Chrome	Смежная сеть	ACE	2026-04-29	✓
41	Высокая	CVE-2026-7335	Google Chrome	Сетевой	ACE	2026-04-29	✓
42	Высокая	CVE-2026-7355	Google Chrome	Сетевой	OSI	2026-04-29	✓
43	Высокая	CVE-2026-7339	Google Chrome	Сетевой	ACE	2026-04-29	✓

44	Высокая	CVE-2026-7348	Google Chrome	Сетевой	ACE	2026-04-29	✓
45	Высокая	CVE-2026-7341	Google Chrome	Сетевой	ACE	2026-04-29	✓
46	Высокая	CVE-2026-7338	Google Chrome	Смежная сеть	ACE	2026-04-29	✓
47	Высокая	CVE-2026-7345	Google Chrome	Сетевой	ACE	2026-04-29	✓
48	Высокая	CVE-2026-7346	Google Chrome	Сетевой	OSI	2026-04-29	✓
49	Высокая	CVE-2026-7347	Google Chrome	Сетевой	ACE	2026-04-29	✓
50	Высокая	CVE-2026-7337	Google Chrome	Сетевой	ACE	2026-04-29	✓
51	Высокая	CVE-2026-7336	Google Chrome	Сетевой	ACE	2026-04-29	✓
52	Высокая	CVE-2026-7342	Google Chrome	Сетевой	ACE	2026-04-29	✓
53	Высокая	CVE-2026-42215	GitPython	Сетевой	ACE	2026-04-27	✓
54	Высокая	CVE-2026-42284	GitPython	Сетевой	ACE	2026-04-27	✓
55	Высокая	CVE-2026-5941	Foxit PDF Reader and PDF Editor for Windows	Локальный	ACE	2026-04-27	✓
56	Высокая	CVE-2026-5943	Foxit PDF Reader and PDF Editor for Windows	Локальный	ACE	2026-04-27	✓
57	Высокая	CVE-2026-5940	Foxit PDF Reader and PDF Editor for Windows	Локальный	ACE	2026-04-27	✓

58	Высокая	CVE-2026-31898	jspdf	Сетевой	CI	2026-04-27	✓
59	Критическая	CVE-2026-31938	jspdf	Сетевой	ACE	2026-04-27	✓
60	Высокая	CVE-2026-25755	jspdf	Сетевой	CI	2026-04-27	✓
61	Высокая	CVE-2026-25535	jspdf	Сетевой	DoS	2026-04-27	✓
62	Высокая	CVE-2026-25940	jspdf	Сетевой	CI	2026-04-27	✓
63	Высокая	CVE-2026-24737	jspdf	Сетевой	CI	2026-04-27	✓
64	Критическая	BDU:2026-04536	Enterprise NFV Infrastructure Software	Сетевой	SB	2026-04-03	✓
65	Критическая	BDU:2026-05530	Cisco Identity Services Engine	Сетевой	ACE	2026-04-17	✓
66	Высокая	BDU:2026-04161	Cisco IOS XE	Сетевой	ACE	2026-03-30	✓
67	Высокая	BDU:2026-05903	Linux	Локальный	DoS	2026-04-20	✓
68	Критическая	BDU:2026-05445	FortiSandbox	Сетевой	ACE	2026-04-15	✓
69	Высокая	BDU:2025-08669	CommuniGate Pro	Сетевой	ACE	2025-07-18	✓
70	Высокая	BDU:2025-01798	CommuniGate Pro	Сетевой	ACE	2025-05-15	✓
71	Критическая	BDU:2025-02495	CommuniGate Pro	Сетевой	ACE	2025-05-16	✓
72	Критическая	BDU:2025-05291	CommuniGate Pro	Сетевой	ACE	2025-05-07	✓

73	Критическая	BDU:2025-01331	CommuniGate Pro	Сетевой	ACE	2024-12-05	✓
74	Высокая	CVE-2026-5287	Microsoft Edge	Сетевой	ACE	2026-04-03	✓
75	Высокая	CVE-2026-5272	Microsoft Edge	Сетевой	ACE	2026-04-03	✓
76	Критическая	CVE-2026-5289	Microsoft Edge	Сетевой	ACE	2026-04-03	✓
77	Высокая	CVE-2026-5280	Microsoft Edge	Сетевой	ACE	2026-04-03	✓
78	Высокая	CVE-2026-5281	Microsoft Edge	Сетевой	ACE	2026-04-03	✓
79	Высокая	CVE-2026-5277	Microsoft Edge	Сетевой	ACE	2026-04-03	✓
80	Критическая	CVE-2026-5290	Microsoft Edge	Сетевой	ACE	2026-04-03	✓
81	Высокая	CVE-2026-5292	Microsoft Edge	Сетевой	OSI	2026-04-03	✓
82	Высокая	CVE-2026-5274	Microsoft Edge	Сетевой	ACE	2026-04-03	✓
83	Высокая	CVE-2026-5285	Microsoft Edge	Сетевой	ACE	2026-04-03	✓
84	Высокая	CVE-2026-5286	Microsoft Edge	Сетевой	ACE	2026-04-03	✓
85	Высокая	CVE-2026-5284	Microsoft Edge	Сетевой	ACE	2026-04-03	✓
86	Высокая	CVE-2026-5275	Microsoft Edge	Сетевой	ACE	2026-04-03	✓
87	Высокая	CVE-2026-5279	Microsoft Edge	Сетевой	ACE	2026-04-03	✓

88	Критическая	CVE-2026-20093	Cisco Unified Computing System (UCS)	Сетевой	OSI	2026-04-01	✓
89	Критическая	CVE-2026-20160	Cisco Smart Software Manager On-Prem	Сетевой	ACE	2026-04-01	✓
90	Высокая	CVE-2025-61726	Ansible Automation Platform 2.5 packages	Сетевой	DoS	2026-04-01	✓
91	Высокая	CVE-2025-14550	Ansible Automation Platform 2.5 packages	Сетевой	DoS	2026-04-01	✓
92	Высокая	CVE-2026-1285	Ansible Automation Platform 2.5 packages	Сетевой	DoS	2026-04-01	✓
93	Высокая	CVE-2025-69223	Ansible Automation Platform 2.5 packages	Сетевой	DoS	2026-04-01	✓
94	Высокая	CVE-2026-22029	Ansible Automation Platform 2.5 packages	Сетевой	XSS\CSS	2026-04-01	✓
95	Высокая	CVE-2026-23490	Ansible Automation Platform 2.5 packages	Сетевой	DoS	2026-04-01	✓
96	Высокая	CVE-2026-3779	Foxit PDF Editor and Reader for Mac	Локальный	ACE	2026-04-01	✓
97	Высокая	CVE-2026-32929	FUJI Electric V-SFT	Локальный	OSI	2026-04-01	✓
98	Высокая	CVE-2026-32928	FUJI Electric V-SFT	Локальный	ACE	2026-04-01	✓
99	Высокая	CVE-2026-32927	FUJI Electric V-SFT	Локальный	OSI	2026-04-01	✓
100	Высокая	CVE-2026-32926	FUJI Electric V-SFT	Локальный	OSI	2026-04-01	✓
101	Высокая	CVE-2026-32925	FUJI Electric V-SFT	Локальный	ACE	2026-04-01	✓

102	Высокая	CVE-2026-5272	Google Chrome	Сетевой	ACE	2026-04-01	✓
103	Высокая	CVE-2026-5274	Google Chrome	Сетевой	ACE	2026-04-01	✓
104	Высокая	CVE-2026-5275	Google Chrome	Сетевой	ACE	2026-04-01	✓
105	Высокая	CVE-2026-5277	Google Chrome	Сетевой	ACE	2026-04-01	✓
106	Высокая	CVE-2026-5278	Google Chrome	Сетевой	ACE	2026-04-01	✓
107	Высокая	CVE-2026-5279	Google Chrome	Сетевой	ACE	2026-04-01	✓
108	Высокая	CVE-2026-5280	Google Chrome	Сетевой	ACE	2026-04-01	✓
109	Высокая	CVE-2026-5281	Google Chrome	Сетевой	ACE	2026-04-01	✓
110	Высокая	CVE-2026-5282	Google Chrome	Сетевой	OSI	2026-04-01	✓
111	Высокая	CVE-2026-5284	Google Chrome	Сетевой	ACE	2026-04-01	✓
112	Высокая	CVE-2026-5286	Google Chrome	Сетевой	ACE	2026-04-01	✓
113	Высокая	CVE-2026-5287	Google Chrome	Сетевой	ACE	2026-04-01	✓
114	Критическая	CVE-2026-5288	Google Chrome	Сетевой	ACE	2026-04-01	✓
115	Критическая	CVE-2026-5289	Google Chrome	Сетевой	ACE	2026-04-01	✓
116	Критическая	CVE-2026-5290	Google Chrome	Сетевой	ACE	2026-04-01	✓

117	Высокая	CVE-2026-5292	Google Chrome	Сетевой	OSI	2026-04-01	✓
118	Высокая	CVE-2026-5285	Google Chrome	Сетевой	ACE	2026-04-01	✓

1

Краткое описание: Отказ в обслуживании в Cisco IOS XE

Идентификатор уязвимости: BDU:2026-04237

Идентификатор программной ошибки: CWE-230 Некорректная обработка отсутствующих (пустых) значений

Уязвимый продукт: Cisco IOS XE: 17.18.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование структурами данных

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-03-30 / 2026-03-30

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-dos-hnX5KGOm

2

Краткое описание: Выполнение произвольного кода в Cisco Evolved Programmable Network Manager

Идентификатор уязвимости: BDU:2026-04594

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Cisco Evolved Programmable Network Manager: до 8.1.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Обход процесса авторизации

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-02 / 2026-04-02

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-epnm-improp-auth-mUwFWUU3

3

Краткое описание: Выполнение произвольного кода в FortiClientEMS

Идентификатор уязвимости: BDU:2026-04638

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: FortiClientEMS: от 7.4.5 до 7.4.7

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Нарушение авторизации.

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: 2026-04-06 / 2026-04-06

Ссылки на источник:

- https://fortiguard.fortinet.com/psirt/FG-IR-26-099
- https://github.com/0xBlackash/CVE-2026-35616?tab=readme-ov-file

4

Краткое описание: Выполнение произвольного кода в Cisco Webex Centers

Идентификатор уязвимости: BDU:2026-05532

Идентификатор программной ошибки: CWE-295 Некорректная проверка сертификатов

Уязвимый продукт: Cisco Webex Centers: -

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Некорректная проверка сертификатов.

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: 2026-04-16 / 2026-04-16

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webex-cui-cert-8jSZYhWL

5

Краткое описание: Выполнение произвольного кода в Cisco Smart Software Manager On-Prem

Идентификатор уязвимости: BDU:2026-04595

Идентификатор программной ошибки: CWE-668 Возможность несанкционированного доступа к ресурсу

Уязвимый продукт: Cisco Smart Software Manager On-Prem: до 9-202601

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Несанкционированный сбор информации

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: 2026-04-02 / 2026-04-02

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-cli-execution-cHUcWuNr

6

Краткое описание: Выполнение произвольного кода в Cisco Identity Services Engine

Идентификатор уязвимости: BDU:2026-05531

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

Уязвимый продукт: Cisco Identity Services Engine: до 3.4 Patch 4

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-17 / 2026-04-17

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-4fverepv

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: 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

7

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

8	**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:** Прикладное программное обеспечение **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:** 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

9	**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:** Прикладное программное обеспечение **Способ эксплуатации:** Отправка специально сформированных данных. **Последствия эксплуатации:** Получение конфиденциальной информации **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. **Оценка CVSSv3:** 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

10

Краткое описание: Выполнение произвольного кода в GnuTLS

Идентификатор уязвимости: CVE-2026-33845

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: GnuTLS: 3.0 - 3.8.12

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: 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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-1
- https://gitlab.com/gnutls/gnutls/-/issues/1816
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-2
- https://gitlab.com/gnutls/gnutls/-/issues/1848
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-3
- https://gitlab.com/gnutls/gnutls/-/issues/1811
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-4
- https://gitlab.com/gnutls/gnutls/-/issues/1850
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-5
- https://gitlab.com/gnutls/gnutls/-/issues/1803
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-6
- https://gitlab.com/gnutls/gnutls/-/issues/1824

- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-7
- https://gitlab.com/gnutls/gnutls/-/issues/1802
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-8
- https://gitlab.com/gnutls/gnutls/-/issues/1825
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-9
- https://gitlab.com/gnutls/gnutls/-/issues/1766
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-10
- https://gitlab.com/gnutls/gnutls/-/issues/1814
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-11
- https://gitlab.com/gnutls/gnutls/-/issues/1840
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-12
- https://gitlab.com/gnutls/gnutls/-/issues/1801
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-13
- https://gitlab.com/gnutls/gnutls/-/issues/1815

11

Краткое описание: Перезапись произвольных файлов в GnuTLS

Идентификатор уязвимости: CVE-2026-33846

Идентификатор программной ошибки: CWE-130 Некорректная обработка несоответствий параметров длины

Уязвимый продукт: GnuTLS: 3.0 - 3.8.12

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Перезапись произвольных файлов

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

Оценка CVSSv3: 7.5 AV: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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-1
- https://gitlab.com/gnutls/gnutls/-/issues/1816
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-2
- https://gitlab.com/gnutls/gnutls/-/issues/1848
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-3
- https://gitlab.com/gnutls/gnutls/-/issues/1811
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-4
- https://gitlab.com/gnutls/gnutls/-/issues/1850
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-5
- https://gitlab.com/gnutls/gnutls/-/issues/1803
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-6
- https://gitlab.com/gnutls/gnutls/-/issues/1824

- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-7
- https://gitlab.com/gnutls/gnutls/-/issues/1802
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-8
- https://gitlab.com/gnutls/gnutls/-/issues/1825
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-9
- https://gitlab.com/gnutls/gnutls/-/issues/1766
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-10
- https://gitlab.com/gnutls/gnutls/-/issues/1814
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-11
- https://gitlab.com/gnutls/gnutls/-/issues/1840
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-12
- https://gitlab.com/gnutls/gnutls/-/issues/1801
- https://www.gnutls.org/security-new.html#GNUTLS-SA-2026-04-29-13
- https://gitlab.com/gnutls/gnutls/-/issues/1815

12

Краткое описание: Выполнение произвольного кода в Wireshark

Идентификатор уязвимости: CVE-2026-5402

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

Уязвимый продукт: Wireshark: 4.4.0 - 4.6.4

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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://www.wireshark.org/security/wnpa-sec-2026-08.html
- https://www.wireshark.org/security/wnpa-sec-2026-32.html
- https://www.wireshark.org/security/wnpa-sec-2026-31.html
- https://www.wireshark.org/security/wnpa-sec-2026-30.html
- https://www.wireshark.org/security/wnpa-sec-2026-29.html
- https://www.wireshark.org/security/wnpa-sec-2026-28.html
- https://www.wireshark.org/security/wnpa-sec-2026-27.html
- https://www.wireshark.org/security/wnpa-sec-2026-26.html
- https://www.wireshark.org/security/wnpa-sec-2026-25.html
- https://www.wireshark.org/security/wnpa-sec-2026-24.html
- https://www.wireshark.org/security/wnpa-sec-2026-23.html
- https://www.wireshark.org/security/wnpa-sec-2026-22.html

- https://www.wireshark.org/security/wnpa-sec-2026-21.html
- https://www.wireshark.org/security/wnpa-sec-2026-20.html
- https://www.wireshark.org/security/wnpa-sec-2026-19.html
- https://www.wireshark.org/security/wnpa-sec-2026-18.html
- https://www.wireshark.org/security/wnpa-sec-2026-17.html
- https://www.wireshark.org/security/wnpa-sec-2026-16.html
- https://www.wireshark.org/security/wnpa-sec-2026-15.html
- https://www.wireshark.org/security/wnpa-sec-2026-14.html
- https://www.wireshark.org/security/wnpa-sec-2026-13.html
- https://www.wireshark.org/security/wnpa-sec-2026-12.html
- https://www.wireshark.org/security/wnpa-sec-2026-11.html
- https://www.wireshark.org/security/wnpa-sec-2026-10.html
- https://www.wireshark.org/security/wnpa-sec-2026-09.html
- https://www.wireshark.org/security/wnpa-sec-2026-39.html
- https://gitlab.com/wireshark/wireshark/-/issues/21182
- https://www.wireshark.org/security/wnpa-sec-2026-40.html
- https://gitlab.com/wireshark/wireshark/-/issues/21181
- https://www.wireshark.org/security/wnpa-sec-2026-41.html
- https://gitlab.com/wireshark/wireshark/-/issues/21184
- https://www.wireshark.org/security/wnpa-sec-2026-42.html
- https://gitlab.com/wireshark/wireshark/-/issues/21186
- https://www.wireshark.org/security/wnpa-sec-2026-43.html
- https://gitlab.com/wireshark/wireshark/-/issues/21189
- https://www.wireshark.org/security/wnpa-sec-2026-44.html
- https://gitlab.com/wireshark/wireshark/-/issues/21190
- https://www.wireshark.org/security/wnpa-sec-2026-45.html
- https://gitlab.com/wireshark/wireshark/-/issues/21191
- https://www.wireshark.org/security/wnpa-sec-2026-46.html
- https://gitlab.com/wireshark/wireshark/-/issues/21185
- https://www.wireshark.org/security/wnpa-sec-2026-47.html
- https://gitlab.com/wireshark/wireshark/-/issues/21214
- https://www.wireshark.org/security/wnpa-sec-2026-48.html
- https://gitlab.com/wireshark/wireshark/-/issues/21206
- https://www.wireshark.org/security/wnpa-sec-2026-34.html

- https://gitlab.com/wireshark/wireshark/-/issues/21149
- https://www.wireshark.org/security/wnpa-sec-2026-37.html
- https://gitlab.com/wireshark/wireshark/-/issues/21172
- https://www.wireshark.org/security/wnpa-sec-2026-38.html
- https://gitlab.com/wireshark/wireshark/-/issues/21177
- https://www.wireshark.org/security/wnpa-sec-2026-49.html
- https://gitlab.com/wireshark/wireshark/-/issues/21207
- https://www.wireshark.org/security/wnpa-sec-2026-50.html
- https://gitlab.com/wireshark/wireshark/-/issues/21130
- https://www.wireshark.org/security/wnpa-sec-2026-33.html
- https://gitlab.com/wireshark/wireshark/-/issues/21151
- https://gitlab.com/wireshark/wireshark/-/issues/21147
- https://www.wireshark.org/security/wnpa-sec-2026-35.html
- https://gitlab.com/wireshark/wireshark/-/issues/21173
- https://www.wireshark.org/security/wnpa-sec-2026-36.html
- https://gitlab.com/wireshark/wireshark/-/issues/21008

13

Краткое описание: Отказ в обслуживании в Wireshark

Идентификатор уязвимости: CVE-2026-5403

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Wireshark: 4.4.0 - 4.6.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://www.wireshark.org/security/wnpa-sec-2026-08.html
- https://www.wireshark.org/security/wnpa-sec-2026-32.html
- https://www.wireshark.org/security/wnpa-sec-2026-31.html
- https://www.wireshark.org/security/wnpa-sec-2026-30.html
- https://www.wireshark.org/security/wnpa-sec-2026-29.html
- https://www.wireshark.org/security/wnpa-sec-2026-28.html
- https://www.wireshark.org/security/wnpa-sec-2026-27.html
- https://www.wireshark.org/security/wnpa-sec-2026-26.html
- https://www.wireshark.org/security/wnpa-sec-2026-25.html
- https://www.wireshark.org/security/wnpa-sec-2026-24.html
- https://www.wireshark.org/security/wnpa-sec-2026-23.html
- https://www.wireshark.org/security/wnpa-sec-2026-22.html

- https://www.wireshark.org/security/wnpa-sec-2026-21.html
- https://www.wireshark.org/security/wnpa-sec-2026-20.html
- https://www.wireshark.org/security/wnpa-sec-2026-19.html
- https://www.wireshark.org/security/wnpa-sec-2026-18.html
- https://www.wireshark.org/security/wnpa-sec-2026-17.html
- https://www.wireshark.org/security/wnpa-sec-2026-16.html
- https://www.wireshark.org/security/wnpa-sec-2026-15.html
- https://www.wireshark.org/security/wnpa-sec-2026-14.html
- https://www.wireshark.org/security/wnpa-sec-2026-13.html
- https://www.wireshark.org/security/wnpa-sec-2026-12.html
- https://www.wireshark.org/security/wnpa-sec-2026-11.html
- https://www.wireshark.org/security/wnpa-sec-2026-10.html
- https://www.wireshark.org/security/wnpa-sec-2026-09.html
- https://www.wireshark.org/security/wnpa-sec-2026-39.html
- https://gitlab.com/wireshark/wireshark/-/issues/21182
- https://www.wireshark.org/security/wnpa-sec-2026-40.html
- https://gitlab.com/wireshark/wireshark/-/issues/21181
- https://www.wireshark.org/security/wnpa-sec-2026-41.html
- https://gitlab.com/wireshark/wireshark/-/issues/21184
- https://www.wireshark.org/security/wnpa-sec-2026-42.html
- https://gitlab.com/wireshark/wireshark/-/issues/21186
- https://www.wireshark.org/security/wnpa-sec-2026-43.html
- https://gitlab.com/wireshark/wireshark/-/issues/21189
- https://www.wireshark.org/security/wnpa-sec-2026-44.html
- https://gitlab.com/wireshark/wireshark/-/issues/21190
- https://www.wireshark.org/security/wnpa-sec-2026-45.html
- https://gitlab.com/wireshark/wireshark/-/issues/21191
- https://www.wireshark.org/security/wnpa-sec-2026-46.html
- https://gitlab.com/wireshark/wireshark/-/issues/21185
- https://www.wireshark.org/security/wnpa-sec-2026-47.html
- https://gitlab.com/wireshark/wireshark/-/issues/21214
- https://www.wireshark.org/security/wnpa-sec-2026-48.html
- https://gitlab.com/wireshark/wireshark/-/issues/21206
- https://www.wireshark.org/security/wnpa-sec-2026-34.html

- https://gitlab.com/wireshark/wireshark/-/issues/21149
- https://www.wireshark.org/security/wnpa-sec-2026-37.html
- https://gitlab.com/wireshark/wireshark/-/issues/21172
- https://www.wireshark.org/security/wnpa-sec-2026-38.html
- https://gitlab.com/wireshark/wireshark/-/issues/21177
- https://www.wireshark.org/security/wnpa-sec-2026-49.html
- https://gitlab.com/wireshark/wireshark/-/issues/21207
- https://www.wireshark.org/security/wnpa-sec-2026-50.html
- https://gitlab.com/wireshark/wireshark/-/issues/21130
- https://www.wireshark.org/security/wnpa-sec-2026-33.html
- https://gitlab.com/wireshark/wireshark/-/issues/21151
- https://gitlab.com/wireshark/wireshark/-/issues/21147
- https://www.wireshark.org/security/wnpa-sec-2026-35.html
- https://gitlab.com/wireshark/wireshark/-/issues/21173
- https://www.wireshark.org/security/wnpa-sec-2026-36.html
- https://gitlab.com/wireshark/wireshark/-/issues/21008

14

Краткое описание: Отказ в обслуживании в Wireshark

Идентификатор уязвимости: CVE-2026-5405

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Wireshark: 4.4.0 - 4.6.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://www.wireshark.org/security/wnpa-sec-2026-08.html
- https://www.wireshark.org/security/wnpa-sec-2026-32.html
- https://www.wireshark.org/security/wnpa-sec-2026-31.html
- https://www.wireshark.org/security/wnpa-sec-2026-30.html
- https://www.wireshark.org/security/wnpa-sec-2026-29.html
- https://www.wireshark.org/security/wnpa-sec-2026-28.html
- https://www.wireshark.org/security/wnpa-sec-2026-27.html
- https://www.wireshark.org/security/wnpa-sec-2026-26.html
- https://www.wireshark.org/security/wnpa-sec-2026-25.html
- https://www.wireshark.org/security/wnpa-sec-2026-24.html
- https://www.wireshark.org/security/wnpa-sec-2026-23.html
- https://www.wireshark.org/security/wnpa-sec-2026-22.html

- https://www.wireshark.org/security/wnpa-sec-2026-21.html
- https://www.wireshark.org/security/wnpa-sec-2026-20.html
- https://www.wireshark.org/security/wnpa-sec-2026-19.html
- https://www.wireshark.org/security/wnpa-sec-2026-18.html
- https://www.wireshark.org/security/wnpa-sec-2026-17.html
- https://www.wireshark.org/security/wnpa-sec-2026-16.html
- https://www.wireshark.org/security/wnpa-sec-2026-15.html
- https://www.wireshark.org/security/wnpa-sec-2026-14.html
- https://www.wireshark.org/security/wnpa-sec-2026-13.html
- https://www.wireshark.org/security/wnpa-sec-2026-12.html
- https://www.wireshark.org/security/wnpa-sec-2026-11.html
- https://www.wireshark.org/security/wnpa-sec-2026-10.html
- https://www.wireshark.org/security/wnpa-sec-2026-09.html
- https://www.wireshark.org/security/wnpa-sec-2026-39.html
- https://gitlab.com/wireshark/wireshark/-/issues/21182
- https://www.wireshark.org/security/wnpa-sec-2026-40.html
- https://gitlab.com/wireshark/wireshark/-/issues/21181
- https://www.wireshark.org/security/wnpa-sec-2026-41.html
- https://gitlab.com/wireshark/wireshark/-/issues/21184
- https://www.wireshark.org/security/wnpa-sec-2026-42.html
- https://gitlab.com/wireshark/wireshark/-/issues/21186
- https://www.wireshark.org/security/wnpa-sec-2026-43.html
- https://gitlab.com/wireshark/wireshark/-/issues/21189
- https://www.wireshark.org/security/wnpa-sec-2026-44.html
- https://gitlab.com/wireshark/wireshark/-/issues/21190
- https://www.wireshark.org/security/wnpa-sec-2026-45.html
- https://gitlab.com/wireshark/wireshark/-/issues/21191
- https://www.wireshark.org/security/wnpa-sec-2026-46.html
- https://gitlab.com/wireshark/wireshark/-/issues/21185
- https://www.wireshark.org/security/wnpa-sec-2026-47.html
- https://gitlab.com/wireshark/wireshark/-/issues/21214
- https://www.wireshark.org/security/wnpa-sec-2026-48.html
- https://gitlab.com/wireshark/wireshark/-/issues/21206
- https://www.wireshark.org/security/wnpa-sec-2026-34.html

- https://gitlab.com/wireshark/wireshark/-/issues/21149
- https://www.wireshark.org/security/wnpa-sec-2026-37.html
- https://gitlab.com/wireshark/wireshark/-/issues/21172
- https://www.wireshark.org/security/wnpa-sec-2026-38.html
- https://gitlab.com/wireshark/wireshark/-/issues/21177
- https://www.wireshark.org/security/wnpa-sec-2026-49.html
- https://gitlab.com/wireshark/wireshark/-/issues/21207
- https://www.wireshark.org/security/wnpa-sec-2026-50.html
- https://gitlab.com/wireshark/wireshark/-/issues/21130
- https://www.wireshark.org/security/wnpa-sec-2026-33.html
- https://gitlab.com/wireshark/wireshark/-/issues/21151
- https://gitlab.com/wireshark/wireshark/-/issues/21147
- https://www.wireshark.org/security/wnpa-sec-2026-35.html
- https://gitlab.com/wireshark/wireshark/-/issues/21173
- https://www.wireshark.org/security/wnpa-sec-2026-36.html
- https://gitlab.com/wireshark/wireshark/-/issues/21008

15

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-4675

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Chrome OS: до 144.0.7559.249

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

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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/long-term-support-channel-update-for_29.html

16

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-4680

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 144.0.7559.249

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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/long-term-support-channel-update-for_29.html

17

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-4456

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 144.0.7559.249

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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/long-term-support-channel-update-for_29.html

18

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2026-6297

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS: до 144.0.7559.249

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: 8.3 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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/long-term-support-channel-update-for_29.html

Краткое описание: Выполнение произвольного кода в FreeBSD

Идентификатор уязвимости: CVE-2026-42511

Идентификатор программной ошибки: CWE-149 Некорректная нейтрализация кавычек

Уязвимый продукт: FreeBSD: 13.5 - 15.0

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

Способ эксплуатации: Некорректная нейтрализация специальных элементов.

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.

19

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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:17.libnv.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:16.libnv.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:15.dhclient.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:14.pf.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:13.exec.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:12.dhclient.asc

Краткое описание: Повышение привилегий в FreeBSD

Идентификатор уязвимости: CVE-2026-7270

Идентификатор программной ошибки: CWE-783 Уязвимость, связанная с приоритетом операторов

Уязвимый продукт: FreeBSD: 13.5 - 15.0

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

Способ эксплуатации: Выполнение специально созданного вредоносного файла

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.

20

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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:17.libnv.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:16.libnv.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:15.dhclient.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:14.pf.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:13.exec.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:12.dhclient.asc

Краткое описание: Отказ в обслуживании в FreeBSD

Идентификатор уязвимости: CVE-2026-7164

Идентификатор программной ошибки: CWE-674 Неконтролируемая рекурсия

Уязвимый продукт: FreeBSD: 13.5 - 15.0

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

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.

21 **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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:17.libnv.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:16.libnv.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:15.dhclient.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:14.pf.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:13.exec.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:12.dhclient.asc

Краткое описание: Выполнение произвольного кода в FreeBSD

Идентификатор уязвимости: CVE-2026-42512

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

Уязвимый продукт: FreeBSD: 13.5 - 15.0

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

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

22

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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:17.libnv.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:16.libnv.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:15.dhclient.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:14.pf.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:13.exec.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:12.dhclient.asc

Краткое описание: Повышение привилегий в FreeBSD

Идентификатор уязвимости: CVE-2026-39457

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: FreeBSD: 13.5 - 15.0

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

Способ эксплуатации: Не определено

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.

23

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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:17.libnv.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:16.libnv.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:15.dhclient.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:14.pf.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:13.exec.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:12.dhclient.asc

Краткое описание: Повышение привилегий в FreeBSD

Идентификатор уязвимости: CVE-2026-35547

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

Уязвимый продукт: FreeBSD: 13.5 - 15.0

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

Способ эксплуатации: Отправка специально сформированных данных.

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.

24

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: 2026-04-30 / 2026-04-30

Ссылки на источник:

- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:17.libnv.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:16.libnv.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:15.dhclient.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:14.pf.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:13.exec.asc
- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:12.dhclient.asc

25

Краткое описание: Получение конфиденциальной информации в SonicOS

Идентификатор уязвимости: CVE-2026-0204

Идентификатор программной ошибки: CWE-306 Отсутствие аутентификации для критически важных функций

Уязвимый продукт: SonicOS: 6.0 - 8.1.0-8017

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Обход процесса аутентификации

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2026-0004
- https://www.sonicwall.com/support/notices/security-advisory-firmware-update-required-gen-6-gen-7-and-gen-8-firewalls/kA1VN000001F03x0AC

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7352

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

26

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7353

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

27

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

28

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7354

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

29

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7356

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7357

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

30

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7350

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

31

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7334

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

32

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

33

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7359

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

34

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7333

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7343

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

35

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7344

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

36

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7361

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

37

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

38

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7358

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

39

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7363

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7349

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

Оценка CVSSv4: Не определено

40

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

41

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7335

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

42

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7355

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

43

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7339

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7348

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

44

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7341

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

45

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7338

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

Оценка CVSSv4: Не определено

46

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7345

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

47

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

48

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-7346

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7347

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

Оценка CVSSv4: Не определено

49

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7337

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

50

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7336

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

51

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-7342

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 147.0.7727.119

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

52

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-29 / 2026-04-29

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/04/stable-channel-update-for-desktop_28.html
- https://crbug.com/503889643
- https://crbug.com/500767595
- https://crbug.com/500880819
- https://crbug.com/501722605
- https://crbug.com/502206907
- https://crbug.com/502248774
- https://crbug.com/502449857
- https://crbug.com/504586599
- https://crbug.com/500104917
- https://crbug.com/493957495
- https://crbug.com/497896137

- https://crbug.com/498285711
- https://crbug.com/500387779
- https://crbug.com/500034684
- https://crbug.com/494352590
- https://crbug.com/496285281
- https://crbug.com/493221953
- https://crbug.com/503419515
- https://crbug.com/503645680
- https://crbug.com/493955227
- https://crbug.com/495852034
- https://crbug.com/496284494
- https://crbug.com/496456528
- https://crbug.com/500018484
- https://crbug.com/497047552
- https://crbug.com/497769116
- https://crbug.com/498746519
- https://crbug.com/498809718
- https://crbug.com/499023054
- https://crbug.com/499119490

53

Краткое описание: Выполнение произвольного кода в GitPython

Идентификатор уязвимости: CVE-2026-42215

Идентификатор программной ошибки: Не определено

Уязвимый продукт: GitPython: 0.1.4 - 3.1.46

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Некорректная нейтрализация специальных элементов.

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: 2026-04-27 / 2026-04-27

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-x2qx-6953-8485
- https://github.com/advisories/GHSA-x2qx-6953-8485
- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-rpm5-65cw-6hj4

54

Краткое описание: Выполнение произвольного кода в GitPython

Идентификатор уязвимости: CVE-2026-42284

Идентификатор программной ошибки: Не определено

Уязвимый продукт: GitPython: 0.1.4 - 3.1.46

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-04-27 / 2026-04-27

Ссылки на источник:

- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-x2qx-6953-8485
- https://github.com/advisories/GHSA-x2qx-6953-8485
- https://github.com/gitpython-developers/GitPython/security/advisories/GHSA-rpm5-65cw-6hj4

55

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

Идентификатор уязвимости: CVE-2026-5941

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): 13.0.0.21632 - 2026.1.0.36452
Foxit PDF Reader for Windows: 2023.2.0.21408 - 2026.1.0.36452

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-04-27 / 2026-04-27

Ссылки на источник:

- https://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+13.2.42026-04-27+00%3A00%3A00
- https://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+2026.1.1+and+Foxit+PDF+Editor+2026.1.1%2F14.0.42026-04-27+00%3A00%3A00

56

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

Идентификатор уязвимости: CVE-2026-5943

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): 13.0.0.21632 - 2026.1.0.36452
Foxit PDF Reader for Windows: 2023.2.0.21408 - 2026.1.0.36452

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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: 2026-04-27 / 2026-04-27

Ссылки на источник:

- https://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+13.2.42026-04-27+00%3A00%3A00
- https://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+2026.1.1+and+Foxit+PDF+Editor+2026.1.1%2F14.0.42026-04-27+00%3A00%3A00

57

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

Идентификатор уязвимости: CVE-2026-5940

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Foxit PDF Editor (formerly Foxit PhantomPDF): 13.0.0.21632 - 2026.1.0.36452
Foxit PDF Reader for Windows: 2023.2.0.21408 - 2026.1.0.36452

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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: 2026-04-27 / 2026-04-27

Ссылки на источник:

- https://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+13.2.42026-04-27+00%3A00%3A00
- https://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+2026.1.1+and+Foxit+PDF+Editor+2026.1.1%2F14.0.42026-04-27+00%3A00%3A00

58

Краткое описание: Внедрение кода в jspdf

Идентификатор уязвимости: CVE-2026-31898

Идентификатор программной ошибки: CWE-116 Некорректная кодировка или очистка выходных данных

Уязвимый продукт: jspdf: 0.9.0 - 4.2.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Внедрение кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-27 / 2026-04-27

Ссылки на источник:

- https://github.com/parallax/jsPDF/security/advisories/GHSA-wfv2-pwc8-crg5
- https://github.com/parallax/jsPDF/security/advisories/GHSA-7x6v-j9x4-qf24

59

Краткое описание: Выполнение произвольного кода в jspdf

Идентификатор уязвимости: CVE-2026-31938

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

Уязвимый продукт: jspdf: 0.9.0 - 4.2.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Некорректная нейтрализация специальных элементов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.6 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-27 / 2026-04-27

Ссылки на источник:

- https://github.com/parallax/jsPDF/security/advisories/GHSA-wfv2-pwc8-crg5
- https://github.com/parallax/jsPDF/security/advisories/GHSA-7x6v-j9x4-qf24

Краткое описание: Внедрение кода в jspdf

Идентификатор уязвимости: CVE-2026-25755

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

Уязвимый продукт: jspdf: 0.9.0 - 4.1.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Внедрение 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.

60 **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: 2026-04-27 / 2026-04-27

Ссылки на источник:

- https://github.com/parallax/jsPDF/security/advisories/GHSA-p5xg-68wr-hm3m
- https://github.com/advisories/GHSA-p5xg-68wr-hm3m
- https://github.com/parallax/jsPDF/security/advisories/GHSA-67pg-wm7f-q7fj
- https://github.com/ZeroXJacks/CVEs/blob/main/2026/CVE-2026-25535.md
- https://github.com/parallax/jsPDF/security/advisories/GHSA-9vjf-qc39-jprp
- https://github.com/ZeroXJacks/CVEs/blob/main/2026/CVE-2026-25755.md

Краткое описание: Отказ в обслуживании в jspdf

Идентификатор уязвимости: CVE-2026-25535

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

Уязвимый продукт: jspdf: 0.9.0 - 4.1.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

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.

61

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

Оценка CVSSv4: 8.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-27 / 2026-04-27

Ссылки на источник:

- https://github.com/parallax/jsPDF/security/advisories/GHSA-p5xg-68wr-hm3m
- https://github.com/advisories/GHSA-p5xg-68wr-hm3m
- https://github.com/parallax/jsPDF/security/advisories/GHSA-67pg-wm7f-q7fj
- https://github.com/ZeroXJacks/CVEs/blob/main/2026/CVE-2026-25535.md
- https://github.com/parallax/jsPDF/security/advisories/GHSA-9vjf-qc39-jprp
- https://github.com/ZeroXJacks/CVEs/blob/main/2026/CVE-2026-25755.md

Краткое описание: Внедрение кода в jspdf

Идентификатор уязвимости: CVE-2026-25940

Идентификатор программной ошибки: CWE-116 Некорректная кодировка или очистка выходных данных

Уязвимый продукт: jspdf: 0.9.0 - 4.1.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Внедрение 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.

62

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: 2026-04-27 / 2026-04-27

Ссылки на источник:

- https://github.com/parallax/jsPDF/security/advisories/GHSA-p5xg-68wr-hm3m
- https://github.com/advisories/GHSA-p5xg-68wr-hm3m
- https://github.com/parallax/jsPDF/security/advisories/GHSA-67pg-wm7f-q7fj
- https://github.com/ZeroXJacks/CVEs/blob/main/2026/CVE-2026-25535.md
- https://github.com/parallax/jsPDF/security/advisories/GHSA-9vjf-qc39-jprp
- https://github.com/ZeroXJacks/CVEs/blob/main/2026/CVE-2026-25755.md

Краткое описание: Внедрение кода в jspdf

Идентификатор уязвимости: CVE-2026-24737

Идентификатор программной ошибки: CWE-116 Некорректная кодировка или очистка выходных данных

Уязвимый продукт: jspdf: 0.9.0 - 4.0.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Внедрение 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.

63 **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: 2026-04-27 / 2026-04-27

Ссылки на источник:

- https://github.com/parallax/jsPDF/security/advisories/GHSA-pqxr-3g65-p328
- https://github.com/parallax/jsPDF/security/advisories/GHSA-vm32-vv63-w422
- https://github.com/advisories/GHSA-vm32-vv63-w422
- https://github.com/parallax/jsPDF/security/advisories/GHSA-95fx-jjr5-f39c
- https://github.com/parallax/jsPDF/security/advisories/GHSA-cjw8-79x6-5cj4
- https://github.com/advisories/GHSA-cjw8-79x6-5cj4

64

Краткое описание: Обход безопасности в Enterprise NFV Infrastructure Software

Идентификатор уязвимости: BDU:2026-04536

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Enterprise NFV Infrastructure Software: 4.16
Integrated Management Controller: до 6.0(1.250174)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 9.8 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: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn

65

Краткое описание: Выполнение произвольного кода в Cisco Identity Services Engine

Идентификатор уязвимости: BDU:2026-05530

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

Уязвимый продукт: Cisco Identity Services Engine: до 3.4 Patch 4

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Манипулирование ресурсами

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-17 / 2026-04-17

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-4fverepv

66

Краткое описание: Выполнение произвольного кода в Cisco IOS XE

Идентификатор уязвимости: BDU:2026-04161

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

Уязвимый продукт: Cisco IOS XE: 17.18.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-03-30 / 2026-03-30

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bootp-WuBhNBxA

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: BDU:2026-05903

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.4 до 6.4.16
Ubuntu: 22.04 LTS
Debian GNU/Linux: 12
Platform V SberLinux OS Server: до 9.2.0-fstec

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

Способ эксплуатации: Использование памяти после ее освобождения

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.

67

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: 2026-04-20 / 2026-04-20

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2025100104-CVE-2023-53454-5ee6@gregkh/
- https://git.kernel.org/stable/c/15ec7cb55e7d88755aa01d44a7a1015a42bfce86
- https://git.kernel.org/stable/c/1d7833db9fd118415dace2ca157bfa603dec9c8c
- https://git.kernel.org/stable/c/2763732ec1e68910719c75b6b896e11b6d3d622b
- https://git.kernel.org/stable/c/39c70c19456e50dcb3abfe53539220dff0490f1d
- https://git.kernel.org/stable/c/4794394635293a3e74591351fff469cea7ad15a2
- https://git.kernel.org/stable/c/ac0d389402a6ff9ad92cea02c2d8c711483b91ab
- https://git.kernel.org/stable/c/b70ac7849248ec8128fa12f86e3655ba38838f29
- https://git.kernel.org/stable/c/dde88ab4e45beb60b217026207aa9c14c88d71ab

- https://git.kernel.org/stable/c/df7ca43fe090e1a56c216c8ebc106ef5fd49afc6
- https://security-tracker.debian.org/tracker/CVE-2023-53454
- https://ubuntu.com/security/CVE-2023-53454

68

Краткое описание: Выполнение произвольного кода в FortiSandbox

Идентификатор уязвимости: BDU:2026-05445

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

Уязвимый продукт: FortiSandbox: от 4.4.0 до 4.4.8 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-15 / 2026-04-15

Ссылки на источник:

- https://fortiguard.fortinet.com/psirt/FG-IR-26-100
- https://github.com/samu-delucas/CVE-2026-39808

69

Краткое описание: Выполнение произвольного кода в CommuniGate Pro

Идентификатор уязвимости: BDU:2025-08669

Идентификатор программной ошибки: CWE-306 Отсутствие аутентификации для критически важных функций

Уязвимый продукт: CommuniGate Pro: 6.5.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение аутентификации.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-18 / 2025-07-18

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-08669

70

Краткое описание: Выполнение произвольного кода в CommuniGate Pro

Идентификатор уязвимости: BDU:2025-01798

Идентификатор программной ошибки: CWE-918 Подделка запроса со стороны сервера

Уязвимый продукт: CommuniGate Pro: до 6.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2025-05-15 / 2025-09-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-01798

71

Краткое описание: Выполнение произвольного кода в CommuniGate Pro

Идентификатор уязвимости: BDU:2025-02495

Идентификатор программной ошибки: CWE-191 Потеря значимости целых чисел (простой или циклический возврат)

Уязвимый продукт: CommuniGate Pro: до 6.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами 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: 2025-05-16 / 2025-08-13

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-02495

72

Краткое описание: Выполнение произвольного кода в CommuniGate Pro

Идентификатор уязвимости: BDU:2025-05291

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

Уязвимый продукт: CommuniGate Pro: до 6.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная нейтрализация специальных элементов.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-05-07 / 2025-05-07

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-05291

73

Краткое описание: Выполнение произвольного кода в CommuniGate Pro

Идентификатор уязвимости: BDU:2025-01331

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: CommuniGate Pro: от 6.3.0 до 6.3.39

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

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: 2024-12-05 / 2024-12-05

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-01331

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5287

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

74

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5272

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

75

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5289

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.6 AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

76

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

77

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5280

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

78

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5281

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

79

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5277

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

80

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5290

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.6 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: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

81

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5292

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

82

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5274

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5285

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

83

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

84

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5286

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5284

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

85

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5275

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

86

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

87

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-5279

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 146.0.3856.84

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-04-03 / 2026-04-03

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5279
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5275
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5284
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5286
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5285
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5274
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5291
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5292
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5273
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5290
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5277

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5281
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5280
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5289
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5272
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5283
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5287
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-5276

88

Краткое описание: Получение конфиденциальной информации в Cisco Unified Computing System (UCS)

Идентификатор уязвимости: CVE-2026-20093

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Cisco Unified Computing System (UCS): до 4.3(6f)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwq55648
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwq55659
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwq68912

89

Краткое описание: Выполнение произвольного кода в Cisco Smart Software Manager On-Prem

Идентификатор уязвимости: CVE-2026-20160

Идентификатор программной ошибки: CWE-668 Возможность несанкционированного доступа к ресурсу

Уязвимый продукт: Cisco Smart Software Manager On-Prem: до 9-202601

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-priv-esc-xRAnOuO8
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwr86065
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ssm-cli-execution-cHUcWuNr
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCws84279

90	**Краткое описание:** Отказ в обслуживании в Ansible Automation Platform 2.5 packages **Идентификатор уязвимости:** CVE-2025-61726 **Идентификатор программной ошибки:** CWE-770 Выделение ресурсов без ограничений или регулировки **Уязвимый продукт:** python3.12-django-storages (Red Hat package): до 1.14.2-3.el8ap python3.12-azure-storage-blob (Red Hat package): до 12.19.0-2.el8ap yamllint (Red Hat package): до 1.35.1-2.el8ap uwsgi (Red Hat package): до 2.0.28-2.el8ap supervisor (Red Hat package): до 4.2.5-2.el8ap receptor (Red Hat package): до 1.6.3-4.el8ap python3.12-zope-interface (Red Hat package): до 6.1-2.el8ap python3.12-zipp (Red Hat package): до 3.19.2-2.el8ap python3.12-yarl (Red Hat package): до 1.18.3-1.el8ap python3.12-xxhash (Red Hat package): до 3.4.1-2.el8ap python3.12-xmlsec (Red Hat package): до 1.3.13-3.el8ap python3.12-xlwt (Red Hat package): до 1.3.0-5.el8ap python3.12-xlrd (Red Hat package): до 2.0.1-7.el8ap python3.12-xds-protos (Red Hat package): до 1.71.2-1.el8ap python3.12-wrapt (Red Hat package): до 1.16.0-2.el8ap python3.12-whitenoise (Red Hat package): до 6.6.0-2.el8ap python3.12-werkzeug (Red Hat package): до 3.0.3-2.el8ap python3.12-websockets (Red Hat package): до 15.0-3.el8ap python3.12-websocket-client (Red Hat package): до 1.7.0-3.el8ap python3.12-wcmatch (Red Hat package): до 8.5-2.el8ap python3.12-watchdog (Red Hat package): до 5.0.2-2.el8ap python3.12-virtualenv (Red Hat package): до 20.25.1-2.el8ap python3.12-validators (Red Hat package): до 0.34.0-2.el8ap python3.12-uuid6 (Red Hat package): до 2024.1.12-2.el8ap python3.12-urllib3 (Red Hat package): до 2.6.3-2.el8ap python3.12-url-normalize (Red Hat package): до 1.4.3-6.el8ap python3.12-uritemplate (Red Hat package): до 4.1.1-4.el8ap python3.12-uamqp (Red Hat package): до 1.6.8-2.el8ap python3.12-typing-extensions (Red Hat package): до 4.15.0-2.el8ap python3.12-txaio (Red Hat package): до 23.1.1-3.el8ap

python3.12-twisted (Red Hat package): до 24.7.0-2.el8ap
python3.12-tox-ansible (Red Hat package): до 25.12.0-2.el8ap
python3.12-tox (Red Hat package): до 4.15.1-2.el8ap
python3.12-termcolor (Red Hat package): до 3.1.0-2.el8ap
python3.12-tacacs-plus (Red Hat package): до 2.6-3.el8ap
python3.12-tabulate (Red Hat package): до 0.9.0-4.el8ap
python3.12-tablib (Red Hat package): до 3.5.0-2.el8ap
python3.12-subprocess-tee (Red Hat package): до 0.4.2-2.el8ap
python3.12-sqlparse (Red Hat package): до 0.5.3-3.el8ap
python3.12-social-auth-core (Red Hat package): до 4.5.4-2.el8ap
python3.12-social-auth-app-django (Red Hat package): до 5.4.1-2.el8ap
python3.12-smmap (Red Hat package): до 5.0.1-2.el8ap
python3.12-six (Red Hat package): до 1.17.0-1.el8ap
python3.12-service-identity (Red Hat package): до 21.1.0-3.el8ap
python3.12-semantic-version (Red Hat package): до 2.10.0-3.el8ap
python3.12-s3transfer (Red Hat package): до 0.10.0-2.el8ap
python3.12-ruamel-yaml-clib (Red Hat package): до 0.2.15-2.el8ap
python3.12-ruamel-yaml (Red Hat package): до 0.18.15-2.el8ap
python3.12-rsa (Red Hat package): до 4.9-3.el8ap
python3.12-rq-scheduler (Red Hat package): до 0.14.0-1.el8ap
python3.12-rq (Red Hat package): до 2.6.1-1.el8ap
python3.12-rpds-py (Red Hat package): до 0.18.1-3.el8ap
python3.12-rich (Red Hat package): до 13.1.0-2.el8ap
python3.12-rfc3339-validator (Red Hat package): до 0.1.4-2.el8ap
python3.12-resolvelib (Red Hat package): до 1.0.1-2.el8ap
python3.12-requests-oauthlib (Red Hat package): до 1.3.1-2.el8ap
python3.12-requests (Red Hat package): до 2.31.0-4.el8ap
python3.12-referencing (Red Hat package): до 0.36.2-3.el8ap
python3.12-redis (Red Hat package): до 4.6.0-3.el8ap
python3.12-pytz (Red Hat package): до 2024.1-2.el8ap
python3.12-python3-saml (Red Hat package): до 1.16.0-3.el8ap
python3.12-python3-openid (Red Hat package): до 3.2.0-4.el8ap
python3.12-pytest-xdist (Red Hat package): до 3.8.0-2.el8ap
python3.12-pytest-sugar (Red Hat package): до 1.1.1-2.el8ap

python3.12-pytest-plus (Red Hat package): до 0.8.1-2.el8ap
python3.12-pytest-ansible (Red Hat package): до 25.12.0-2.el8ap
python3.12-pytest (Red Hat package): до 9.0.1-2.el8ap
python3.12-pyrad (Red Hat package): до 2.4-3.el8ap
python3.12-pyproject-api (Red Hat package): до 1.6.1-2.el8ap
python3.12-pyparsing (Red Hat package): до 3.1.1-2.el8ap
python3.12-pyjwt (Red Hat package): до 2.7.0-3.el8ap
python3.12-pygtrie (Red Hat package): до 2.5.0-3.el8ap
python3.12-pygments (Red Hat package): до 2.17.2-3.el8ap
python3.12-pyflakes (Red Hat package): до 3.1.0-2.el8ap
python3.12-pydantic (Red Hat package): до 1.10.15-2.el8ap
python3.12-pycodestyle (Red Hat package): до 2.11.1-2.el8ap
python3.12-pycares (Red Hat package): до 4.4.0-3.el8ap
python3.12-pyasn1-modules (Red Hat package): до 0.3.0-2.el8ap
python3.12-pyasn1 (Red Hat package): до 0.5.1-2.el8ap
python3.12-pyOpenSSL (Red Hat package): до 24.1.0-2.el8ap
python3.12-pulpcore (Red Hat package): до 3.49.50-1.el8ap
python3.12-pulp-glue (Red Hat package): до 0.23.2-2.el8ap
python3.12-pulp-container (Red Hat package): до 2.19.3-2.el8ap
python3.12-pulp-ansible (Red Hat package): до 0.25.1-2.el8ap
python3.12-ptyprocess (Red Hat package): до 0.7.0-2.el8ap
python3.12-psycopg (Red Hat package): до 3.2.7-2.el8ap
python3.12-protobuf (Red Hat package): до 5.29.6-1.el8ap
python3.12-propcache (Red Hat package): до 0.4.1-1.el8ap
python3.12-prometheus-client (Red Hat package): до 0.19.0-2.el8ap
python3.12-podman (Red Hat package): до 5.4.0.1-2.el8ap
python3.12-pluggy (Red Hat package): до 1.6.0-2.el8ap
python3.12-platformdirs (Red Hat package): до 4.2.0-2.el8ap
python3.12-pillow (Red Hat package): до 10.3.0-2.el8ap
python3.12-pexpect (Red Hat package): до 4.9.0-2.el8ap
python3.12-persisting-theory (Red Hat package): до 1.0-3.el8ap
python3.12-pbr (Red Hat package): до 6.0.0-3.el8ap
python3.12-pathspec (Red Hat package): до 0.12.1-2.el8ap
python3.12-pathable (Red Hat package): до 0.4.3-2.el8ap

python3.12-parsley (Red Hat package): до 1.3-4.el8ap
python3.12-parse (Red Hat package): до 1.20.1-2.el8ap
python3.12-packaging (Red Hat package): до 23.2-2.el8
python3.12-opentelemetry-contrib (Red Hat package): до 1.28.0-1.el8ap
python3.12-opentelemetry (Red Hat package): до 1.28.0-1.el8ap
python3.12-openpyxl (Red Hat package): до 3.1.2-2.el8ap
python3.12-openapi-spec-validator (Red Hat package): до 0.7.1-2.el8ap
python3.12-openapi-schema-validator (Red Hat package): до 0.6.2-2.el8ap
python3.12-openapi-core (Red Hat package): до 0.19.1-2.el8ap
python3.12-onigurumacffi (Red Hat package): до 1.3.0-2.el8ap
python3.12-odfpy (Red Hat package): до 1.4.1-9.el8ap
python3.12-oauthlib (Red Hat package): до 3.2.2-2.el8ap
python3.12-nh3 (Red Hat package): до 0.2.18-2.el8ap
python3.12-netaddr (Red Hat package): до 1.2.1-2.el8ap
python3.12-mypy-extensions (Red Hat package): до 1.0.0-2.el8ap
python3.12-multidict (Red Hat package): до 6.0.4-2.el8ap
python3.12-more-itertools (Red Hat package): до 10.2.0-2.el8ap
python3.12-mccabe (Red Hat package): до 0.7.0-3.el8ap
python3.12-marshmallow (Red Hat package): до 3.26.2-1.el8ap
python3.12-markupsafe (Red Hat package): до 2.1.5-2.el8ap
python3.12-markuppy (Red Hat package): до 1.14-5.el8ap
python3.12-markdown (Red Hat package): до 3.5.2-2.el8ap
python3.12-lxml (Red Hat package): до 5.3.0-2.el8ap
python3.12-lockfile (Red Hat package): до 0.12.2-3.el8ap
python3.12-ldap-filter (Red Hat package): до 1.0.1-2.el8ap
python3.12-ldap (Red Hat package): до 3.4.5-1.el8ap
python3.12-lazy-object-proxy (Red Hat package): до 1.10.0-2.el8ap
python3.12-kubernetes (Red Hat package): до 26.1.0-3.el8ap
python3.12-jwcrypto (Red Hat package): до 1.5.6-2.el8ap
python3.12-jsonschema-specifications (Red Hat package): до 2023.12.1-2.el8ap
python3.12-jsonschema-path (Red Hat package): до 0.3.4-2.el8ap
python3.12-jsonschema (Red Hat package): до 4.21.1-2.el8ap
python3.12-json-stream-rs-tokenizer (Red Hat package): до 0.4.26-2.el8ap
python3.12-json-stream (Red Hat package): до 2.3.2-2.el8ap

python3.12-jq (Red Hat package): до 1.6.0-2.el8ap
python3.12-jpy (Red Hat package): до 0.15.0-2.el8ap
python3.12-jmespath (Red Hat package): до 1.0.1-3.el8ap
python3.12-jinja2 (Red Hat package): до 3.1.6-2.el8ap
python3.12-janus (Red Hat package): до 1.0.0-3.el8ap
python3.12-isodate (Red Hat package): до 0.6.1-3.el8ap
python3.12-insights-analytics-collector (Red Hat package): до 0.3.2-3.el8ap
python3.12-iniconfig (Red Hat package): до 2.0.0-2.el8ap
python3.12-inflection (Red Hat package): до 0.5.1-5.el8ap
python3.12-incremental (Red Hat package): до 24.7.2-2.el8ap
python3.12-importlib-metadata (Red Hat package): до 6.0.1-3.el8ap
python3.12-hyperlink (Red Hat package): до 21.0.0-3.el8ap
python3.12-gunicorn (Red Hat package): до 23.0.0-2.el8ap
python3.12-grpcio (Red Hat package): до 1.71.2-1.el8ap
python3.12-googleapis-common-protos (Red Hat package): до 1.72.0-1.el8ap
python3.12-google-auth (Red Hat package): до 2.27.0-2.el8ap
python3.12-gnupg (Red Hat package): до 0.5.2-2.el8ap
python3.12-gitpython (Red Hat package): до 3.1.41-2.el8ap
python3.12-gitdb (Red Hat package): до 4.0.11-2.el8ap
python3.12-galaxy-ng (Red Hat package): до 4.10.12-1.el8ap
python3.12-galaxy-importer (Red Hat package): до 0.4.37-3.el8ap
python3.12-frozenlist (Red Hat package): до 1.4.0-2.el8ap
python3.12-freezegun (Red Hat package): до 1.5.5-1.el8ap
python3.12-flake8 (Red Hat package): до 6.1.0-3.el8ap
python3.12-filelock (Red Hat package): до 3.13.1-2.el8ap
python3.12-execnet (Red Hat package): до 2.1.2-2.el8ap
python3.12-et-xmlfile (Red Hat package): до 1.1.0-4.el8ap
python3.12-enrich (Red Hat package): до 1.2.7-3.el8ap
python3.12-ecdsa (Red Hat package): до 0.18.0-2.el8ap
python3.12-dynaconf (Red Hat package): до 3.2.11-2.el8ap
python3.12-drools-jpy (Red Hat package): до 0.3.10-2.el8ap
python3.12-drf-spectacular (Red Hat package): до 0.26.5-3.el8ap
python3.12-drf-nested-routers (Red Hat package): до 0.93.5-2.el8ap
python3.12-drf-access-policy (Red Hat package): до 1.5.0-2.el8ap

python3.12-dpath (Red Hat package): до 2.1.6-2.el8ap
python3.12-djangorestframework-queryfields (Red Hat package): до 1.1.0-2.el8ap
python3.12-djangorestframework (Red Hat package): до 3.15.1-2.el8ap
python3.12-django-split-settings (Red Hat package): до 1.2.0-3.el8ap
python3.12-django-rq (Red Hat package): до 3.2.2-1.el8ap
python3.12-django-redis (Red Hat package): до 5.4.0-2.el8ap
python3.12-django-prometheus (Red Hat package): до 2.3.1-3.el8ap
python3.12-django-picklefield (Red Hat package): до 3.1-2.el8ap
python3.12-django-oauth-toolkit (Red Hat package): до 2.3.0-2.el8ap
python3.12-django-lifecycle (Red Hat package): до 1.1.2-2.el8ap
python3.12-django-ipware (Red Hat package): до 3.0.7-4.el8ap
python3.12-django-import-export (Red Hat package): до 3.3.6-3.el8ap
python3.12-django-guid (Red Hat package): до 3.4.0-2.el8ap
python3.12-django-flags (Red Hat package): до 5.0.13-2.el8ap
python3.12-django-filter (Red Hat package): до 23.5-2.el8ap
python3.12-django-extensions (Red Hat package): до 4.1-2.el8ap
python3.12-django-dynamic-preferences (Red Hat package): до 1.16.0-2.el8ap
python3.12-django-crum (Red Hat package): до 0.7.9-3.el8ap
python3.12-django-auth-ldap (Red Hat package): до 4.0.0-3.el8ap
python3.12-django-ansible-base (Red Hat package): до 2.5.20260225-1.el8ap
python3.12-django (Red Hat package): до 4.2.28-1.el8ap
python3.12-distro (Red Hat package): до 1.9.0-2.el8ap
python3.12-distlib (Red Hat package): до 0.4.0-2.el8ap
python3.12-dispatcherd (Red Hat package): до 2025.5.19-3.el8ap
python3.12-diff-match-patch (Red Hat package): до 20230430-2.el8ap
python3.12-deprecated (Red Hat package): до 1.2.14-2.el8ap
python3.12-defusedxml (Red Hat package): до 0.7.1-5.el8ap
python3.12-dateutil (Red Hat package): до 2.8.2-3.el8ap
python3.12-daphne (Red Hat package): до 4.0.0-4.el8ap
python3.12-daemon (Red Hat package): до 3.1.2-3.el8ap
python3.12-cryptography (Red Hat package): до 42.0.5-2.el8ap
python3.12-crontab (Red Hat package): до 1.0.5-1.el8ap
python3.12-croniter (Red Hat package): до 2.0.1-2.el8ap
python3.12-constantly (Red Hat package): до 23.10.4-1.el8ap

python3.12-commonmark (Red Hat package): до 0.9.1-7.el8ap
python3.12-colorama (Red Hat package): до 0.4.6-2.el8ap
python3.12-click-help-colors (Red Hat package): до 0.9.4-2.el8ap
python3.12-click (Red Hat package): до 8.1.7-2.el8ap
python3.12-chardet (Red Hat package): до 5.2.0-3.el8ap
python3.12-channels (Red Hat package): до 4.0.0-4.el8ap
python3.12-certifi (Red Hat package): до 2023.5.7-2.el8ap
python3.12-cachetools (Red Hat package): до 5.3.2-2.el8ap
python3.12-brotli (Red Hat package): до 1.2.0-1.el8ap
python3.12-bracex (Red Hat package): до 2.4-2.el8ap
python3.12-botocore (Red Hat package): до 1.34.162-2.el8ap
python3.12-boto3 (Red Hat package): до 1.34.30-2.el8ap
python3.12-black (Red Hat package): до 24.4.2-3.el8ap
python3.12-backoff (Red Hat package): до 2.2.1-2.el8ap
python3.12-azure-core (Red Hat package): до 1.34.0-2.el8ap
python3.12-autobahn (Red Hat package): до 24.4.2-2.el8ap
python3.12-attrs (Red Hat package): до 22.2.0-2.el8ap
python3.12-asyncio-throttle (Red Hat package): до 1.0.2-5.el8ap
python3.12-async-lru (Red Hat package): до 2.0.5-1.el8ap
python3.12-asgiref (Red Hat package): до 3.7.2-2.el8ap
python3.12-argon2-cffi-bindings (Red Hat package): до 21.2.0-2.el8ap
python3.12-argon2-cffi (Red Hat package): до 23.1.0-2.el8ap
python3.12-ansible-sdk (Red Hat package): до 1.0.0-3.el8ap
python3.12-ansible-pylibssh (Red Hat package): до 1.2.2-2.el8ap
python3.12-ansible-compat (Red Hat package): до 25.12.0-3.el8ap
python3.12-aiosignal (Red Hat package): до 1.4.0-1.el8ap
python3.12-aiohttp (Red Hat package): до 3.13.3-2.el8ap
python3.12-aiohappyeyeballs (Red Hat package): до 2.6.1-1.el8ap
python3.12-aiofiles (Red Hat package): до 23.2.1-2.el8ap
python3.12-aiodns (Red Hat package): до 3.2.0-2.el8ap
python3.12-Automat (Red Hat package): до 22.10.0-4.el8ap
pulpcore-selinux (Red Hat package): до 2.0.1-2.el8ap
molecule (Red Hat package): до 25.12.0-2.el8ap
bindep (Red Hat package): до 2.13.0-2.el8ap

automation-hub (Red Hat package): до 4.10.12-1.el8ap
automation-gateway (Red Hat package): до 2.5.20260225-1.el8ap
automation-eda-controller (Red Hat package): до 1.1.16-1.el8ap
automation-controller-fapolicyd (Red Hat package): до 1.0-6.el8ap
automation-controller (Red Hat package): до 4.6.26-1.el8ap
ansible-sign (Red Hat package): до 0.1.4-2.el8ap
ansible-runner (Red Hat package): до 2.4.2-3.el8ap
ansible-rulebook (Red Hat package): до 1.1.7-2.el8ap
ansible-navigator (Red Hat package): до 26.1.1-1.1.el8ap
ansible-lint (Red Hat package): до 26.1.0-3.el8ap
ansible-dev-tools (Red Hat package): до 26.1.0-3.el8ap
ansible-dev-environment (Red Hat package): до 25.12.2-1.2.el8ap
ansible-creator (Red Hat package): до 25.12.0-1.1.el8ap
ansible-core (Red Hat package): до 2.16.16-1.el8ap
ansible-builder (Red Hat package): до 3.1.1-1.2.el8ap
ansible-automation-platform-installer (Red Hat package): до 2.5-21.el8ap
aap-metrics-utility (Red Hat package): до 0.6.0-2.1.el8ap
python3.12-wheel (Red Hat package): до 0.41.2-4.el8_10
python3.12-setuptools (Red Hat package): до 68.2.2-5.el9_6
Ansible Automation Platform: до 2.5

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: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2026:3959

91	**Краткое описание:** Отказ в обслуживании в Ansible Automation Platform 2.5 packages **Идентификатор уязвимости:** CVE-2025-14550 **Идентификатор программной ошибки:** CWE-407 Алгоритмическая сложность **Уязвимый продукт:** python3.12-django-storages (Red Hat package): до 1.14.2-3.el8ap python3.12-azure-storage-blob (Red Hat package): до 12.19.0-2.el8ap yamllint (Red Hat package): до 1.35.1-2.el8ap uwsgi (Red Hat package): до 2.0.28-2.el8ap supervisor (Red Hat package): до 4.2.5-2.el8ap receptor (Red Hat package): до 1.6.3-4.el8ap python3.12-zope-interface (Red Hat package): до 6.1-2.el8ap python3.12-zipp (Red Hat package): до 3.19.2-2.el8ap python3.12-yarl (Red Hat package): до 1.18.3-1.el8ap python3.12-xxhash (Red Hat package): до 3.4.1-2.el8ap python3.12-xmlsec (Red Hat package): до 1.3.13-3.el8ap python3.12-xlwt (Red Hat package): до 1.3.0-5.el8ap python3.12-xlrd (Red Hat package): до 2.0.1-7.el8ap python3.12-xds-protos (Red Hat package): до 1.71.2-1.el8ap python3.12-wrapt (Red Hat package): до 1.16.0-2.el8ap python3.12-whitenoise (Red Hat package): до 6.6.0-2.el8ap python3.12-werkzeug (Red Hat package): до 3.0.3-2.el8ap python3.12-websockets (Red Hat package): до 15.0-3.el8ap python3.12-websocket-client (Red Hat package): до 1.7.0-3.el8ap python3.12-wcmatch (Red Hat package): до 8.5-2.el8ap python3.12-watchdog (Red Hat package): до 5.0.2-2.el8ap python3.12-virtualenv (Red Hat package): до 20.25.1-2.el8ap python3.12-validators (Red Hat package): до 0.34.0-2.el8ap python3.12-uuid6 (Red Hat package): до 2024.1.12-2.el8ap python3.12-urllib3 (Red Hat package): до 2.6.3-2.el8ap python3.12-url-normalize (Red Hat package): до 1.4.3-6.el8ap python3.12-uritemplate (Red Hat package): до 4.1.1-4.el8ap python3.12-uamqp (Red Hat package): до 1.6.8-2.el8ap python3.12-typing-extensions (Red Hat package): до 4.15.0-2.el8ap python3.12-txaio (Red Hat package): до 23.1.1-3.el8ap

python3.12-twisted (Red Hat package): до 24.7.0-2.el8ap
python3.12-tox-ansible (Red Hat package): до 25.12.0-2.el8ap
python3.12-tox (Red Hat package): до 4.15.1-2.el8ap
python3.12-termcolor (Red Hat package): до 3.1.0-2.el8ap
python3.12-tacacs-plus (Red Hat package): до 2.6-3.el8ap
python3.12-tabulate (Red Hat package): до 0.9.0-4.el8ap
python3.12-tablib (Red Hat package): до 3.5.0-2.el8ap
python3.12-subprocess-tee (Red Hat package): до 0.4.2-2.el8ap
python3.12-sqlparse (Red Hat package): до 0.5.3-3.el8ap
python3.12-social-auth-core (Red Hat package): до 4.5.4-2.el8ap
python3.12-social-auth-app-django (Red Hat package): до 5.4.1-2.el8ap
python3.12-smmap (Red Hat package): до 5.0.1-2.el8ap
python3.12-six (Red Hat package): до 1.17.0-1.el8ap
python3.12-service-identity (Red Hat package): до 21.1.0-3.el8ap
python3.12-semantic-version (Red Hat package): до 2.10.0-3.el8ap
python3.12-s3transfer (Red Hat package): до 0.10.0-2.el8ap
python3.12-ruamel-yaml-clib (Red Hat package): до 0.2.15-2.el8ap
python3.12-ruamel-yaml (Red Hat package): до 0.18.15-2.el8ap
python3.12-rsa (Red Hat package): до 4.9-3.el8ap
python3.12-rq-scheduler (Red Hat package): до 0.14.0-1.el8ap
python3.12-rq (Red Hat package): до 2.6.1-1.el8ap
python3.12-rpds-py (Red Hat package): до 0.18.1-3.el8ap
python3.12-rich (Red Hat package): до 13.1.0-2.el8ap
python3.12-rfc3339-validator (Red Hat package): до 0.1.4-2.el8ap
python3.12-resolvelib (Red Hat package): до 1.0.1-2.el8ap
python3.12-requests-oauthlib (Red Hat package): до 1.3.1-2.el8ap
python3.12-requests (Red Hat package): до 2.31.0-4.el8ap
python3.12-referencing (Red Hat package): до 0.36.2-3.el8ap
python3.12-redis (Red Hat package): до 4.6.0-3.el8ap
python3.12-pytz (Red Hat package): до 2024.1-2.el8ap
python3.12-python3-saml (Red Hat package): до 1.16.0-3.el8ap
python3.12-python3-openid (Red Hat package): до 3.2.0-4.el8ap
python3.12-pytest-xdist (Red Hat package): до 3.8.0-2.el8ap
python3.12-pytest-sugar (Red Hat package): до 1.1.1-2.el8ap

python3.12-pytest-plus (Red Hat package): до 0.8.1-2.el8ap
python3.12-pytest-ansible (Red Hat package): до 25.12.0-2.el8ap
python3.12-pytest (Red Hat package): до 9.0.1-2.el8ap
python3.12-pyrad (Red Hat package): до 2.4-3.el8ap
python3.12-pyproject-api (Red Hat package): до 1.6.1-2.el8ap
python3.12-pyparsing (Red Hat package): до 3.1.1-2.el8ap
python3.12-pyjwt (Red Hat package): до 2.7.0-3.el8ap
python3.12-pygtrie (Red Hat package): до 2.5.0-3.el8ap
python3.12-pygments (Red Hat package): до 2.17.2-3.el8ap
python3.12-pyflakes (Red Hat package): до 3.1.0-2.el8ap
python3.12-pydantic (Red Hat package): до 1.10.15-2.el8ap
python3.12-pycodestyle (Red Hat package): до 2.11.1-2.el8ap
python3.12-pycares (Red Hat package): до 4.4.0-3.el8ap
python3.12-pyasn1-modules (Red Hat package): до 0.3.0-2.el8ap
python3.12-pyasn1 (Red Hat package): до 0.5.1-2.el8ap
python3.12-pyOpenSSL (Red Hat package): до 24.1.0-2.el8ap
python3.12-pulpcore (Red Hat package): до 3.49.50-1.el8ap
python3.12-pulp-glue (Red Hat package): до 0.23.2-2.el8ap
python3.12-pulp-container (Red Hat package): до 2.19.3-2.el8ap
python3.12-pulp-ansible (Red Hat package): до 0.25.1-2.el8ap
python3.12-ptyprocess (Red Hat package): до 0.7.0-2.el8ap
python3.12-psycopg (Red Hat package): до 3.2.7-2.el8ap
python3.12-protobuf (Red Hat package): до 5.29.6-1.el8ap
python3.12-propcache (Red Hat package): до 0.4.1-1.el8ap
python3.12-prometheus-client (Red Hat package): до 0.19.0-2.el8ap
python3.12-podman (Red Hat package): до 5.4.0.1-2.el8ap
python3.12-pluggy (Red Hat package): до 1.6.0-2.el8ap
python3.12-platformdirs (Red Hat package): до 4.2.0-2.el8ap
python3.12-pillow (Red Hat package): до 10.3.0-2.el8ap
python3.12-pexpect (Red Hat package): до 4.9.0-2.el8ap
python3.12-persisting-theory (Red Hat package): до 1.0-3.el8ap
python3.12-pbr (Red Hat package): до 6.0.0-3.el8ap
python3.12-pathspec (Red Hat package): до 0.12.1-2.el8ap
python3.12-pathable (Red Hat package): до 0.4.3-2.el8ap

python3.12-parsley (Red Hat package): до 1.3-4.el8ap
python3.12-parse (Red Hat package): до 1.20.1-2.el8ap
python3.12-packaging (Red Hat package): до 23.2-2.el8
python3.12-opentelemetry-contrib (Red Hat package): до 1.28.0-1.el8ap
python3.12-opentelemetry (Red Hat package): до 1.28.0-1.el8ap
python3.12-openpyxl (Red Hat package): до 3.1.2-2.el8ap
python3.12-openapi-spec-validator (Red Hat package): до 0.7.1-2.el8ap
python3.12-openapi-schema-validator (Red Hat package): до 0.6.2-2.el8ap
python3.12-openapi-core (Red Hat package): до 0.19.1-2.el8ap
python3.12-onigurumacffi (Red Hat package): до 1.3.0-2.el8ap
python3.12-odfpy (Red Hat package): до 1.4.1-9.el8ap
python3.12-oauthlib (Red Hat package): до 3.2.2-2.el8ap
python3.12-nh3 (Red Hat package): до 0.2.18-2.el8ap
python3.12-netaddr (Red Hat package): до 1.2.1-2.el8ap
python3.12-mypy-extensions (Red Hat package): до 1.0.0-2.el8ap
python3.12-multidict (Red Hat package): до 6.0.4-2.el8ap
python3.12-more-itertools (Red Hat package): до 10.2.0-2.el8ap
python3.12-mccabe (Red Hat package): до 0.7.0-3.el8ap
python3.12-marshmallow (Red Hat package): до 3.26.2-1.el8ap
python3.12-markupsafe (Red Hat package): до 2.1.5-2.el8ap
python3.12-markuppy (Red Hat package): до 1.14-5.el8ap
python3.12-markdown (Red Hat package): до 3.5.2-2.el8ap
python3.12-lxml (Red Hat package): до 5.3.0-2.el8ap
python3.12-lockfile (Red Hat package): до 0.12.2-3.el8ap
python3.12-ldap-filter (Red Hat package): до 1.0.1-2.el8ap
python3.12-ldap (Red Hat package): до 3.4.5-1.el8ap
python3.12-lazy-object-proxy (Red Hat package): до 1.10.0-2.el8ap
python3.12-kubernetes (Red Hat package): до 26.1.0-3.el8ap
python3.12-jwcrypto (Red Hat package): до 1.5.6-2.el8ap
python3.12-jsonschema-specifications (Red Hat package): до 2023.12.1-2.el8ap
python3.12-jsonschema-path (Red Hat package): до 0.3.4-2.el8ap
python3.12-jsonschema (Red Hat package): до 4.21.1-2.el8ap
python3.12-json-stream-rs-tokenizer (Red Hat package): до 0.4.26-2.el8ap
python3.12-json-stream (Red Hat package): до 2.3.2-2.el8ap

python3.12-jq (Red Hat package): до 1.6.0-2.el8ap
python3.12-jpy (Red Hat package): до 0.15.0-2.el8ap
python3.12-jmespath (Red Hat package): до 1.0.1-3.el8ap
python3.12-jinja2 (Red Hat package): до 3.1.6-2.el8ap
python3.12-janus (Red Hat package): до 1.0.0-3.el8ap
python3.12-isodate (Red Hat package): до 0.6.1-3.el8ap
python3.12-insights-analytics-collector (Red Hat package): до 0.3.2-3.el8ap
python3.12-iniconfig (Red Hat package): до 2.0.0-2.el8ap
python3.12-inflection (Red Hat package): до 0.5.1-5.el8ap
python3.12-incremental (Red Hat package): до 24.7.2-2.el8ap
python3.12-importlib-metadata (Red Hat package): до 6.0.1-3.el8ap
python3.12-hyperlink (Red Hat package): до 21.0.0-3.el8ap
python3.12-gunicorn (Red Hat package): до 23.0.0-2.el8ap
python3.12-grpcio (Red Hat package): до 1.71.2-1.el8ap
python3.12-googleapis-common-protos (Red Hat package): до 1.72.0-1.el8ap
python3.12-google-auth (Red Hat package): до 2.27.0-2.el8ap
python3.12-gnupg (Red Hat package): до 0.5.2-2.el8ap
python3.12-gitpython (Red Hat package): до 3.1.41-2.el8ap
python3.12-gitdb (Red Hat package): до 4.0.11-2.el8ap
python3.12-galaxy-ng (Red Hat package): до 4.10.12-1.el8ap
python3.12-galaxy-importer (Red Hat package): до 0.4.37-3.el8ap
python3.12-frozenlist (Red Hat package): до 1.4.0-2.el8ap
python3.12-freezegun (Red Hat package): до 1.5.5-1.el8ap
python3.12-flake8 (Red Hat package): до 6.1.0-3.el8ap
python3.12-filelock (Red Hat package): до 3.13.1-2.el8ap
python3.12-execnet (Red Hat package): до 2.1.2-2.el8ap
python3.12-et-xmlfile (Red Hat package): до 1.1.0-4.el8ap
python3.12-enrich (Red Hat package): до 1.2.7-3.el8ap
python3.12-ecdsa (Red Hat package): до 0.18.0-2.el8ap
python3.12-dynaconf (Red Hat package): до 3.2.11-2.el8ap
python3.12-drools-jpy (Red Hat package): до 0.3.10-2.el8ap
python3.12-drf-spectacular (Red Hat package): до 0.26.5-3.el8ap
python3.12-drf-nested-routers (Red Hat package): до 0.93.5-2.el8ap
python3.12-drf-access-policy (Red Hat package): до 1.5.0-2.el8ap

python3.12-dpath (Red Hat package): до 2.1.6-2.el8ap
python3.12-djangorestframework-queryfields (Red Hat package): до 1.1.0-2.el8ap
python3.12-djangorestframework (Red Hat package): до 3.15.1-2.el8ap
python3.12-django-split-settings (Red Hat package): до 1.2.0-3.el8ap
python3.12-django-rq (Red Hat package): до 3.2.2-1.el8ap
python3.12-django-redis (Red Hat package): до 5.4.0-2.el8ap
python3.12-django-prometheus (Red Hat package): до 2.3.1-3.el8ap
python3.12-django-picklefield (Red Hat package): до 3.1-2.el8ap
python3.12-django-oauth-toolkit (Red Hat package): до 2.3.0-2.el8ap
python3.12-django-lifecycle (Red Hat package): до 1.1.2-2.el8ap
python3.12-django-ipware (Red Hat package): до 3.0.7-4.el8ap
python3.12-django-import-export (Red Hat package): до 3.3.6-3.el8ap
python3.12-django-guid (Red Hat package): до 3.4.0-2.el8ap
python3.12-django-flags (Red Hat package): до 5.0.13-2.el8ap
python3.12-django-filter (Red Hat package): до 23.5-2.el8ap
python3.12-django-extensions (Red Hat package): до 4.1-2.el8ap
python3.12-django-dynamic-preferences (Red Hat package): до 1.16.0-2.el8ap
python3.12-django-crum (Red Hat package): до 0.7.9-3.el8ap
python3.12-django-auth-ldap (Red Hat package): до 4.0.0-3.el8ap
python3.12-django-ansible-base (Red Hat package): до 2.5.20260225-1.el8ap
python3.12-django (Red Hat package): до 4.2.28-1.el8ap
python3.12-distro (Red Hat package): до 1.9.0-2.el8ap
python3.12-distlib (Red Hat package): до 0.4.0-2.el8ap
python3.12-dispatcherd (Red Hat package): до 2025.5.19-3.el8ap
python3.12-diff-match-patch (Red Hat package): до 20230430-2.el8ap
python3.12-deprecated (Red Hat package): до 1.2.14-2.el8ap
python3.12-defusedxml (Red Hat package): до 0.7.1-5.el8ap
python3.12-dateutil (Red Hat package): до 2.8.2-3.el8ap
python3.12-daphne (Red Hat package): до 4.0.0-4.el8ap
python3.12-daemon (Red Hat package): до 3.1.2-3.el8ap
python3.12-cryptography (Red Hat package): до 42.0.5-2.el8ap
python3.12-crontab (Red Hat package): до 1.0.5-1.el8ap
python3.12-croniter (Red Hat package): до 2.0.1-2.el8ap
python3.12-constantly (Red Hat package): до 23.10.4-1.el8ap

python3.12-commonmark (Red Hat package): до 0.9.1-7.el8ap
python3.12-colorama (Red Hat package): до 0.4.6-2.el8ap
python3.12-click-help-colors (Red Hat package): до 0.9.4-2.el8ap
python3.12-click (Red Hat package): до 8.1.7-2.el8ap
python3.12-chardet (Red Hat package): до 5.2.0-3.el8ap
python3.12-channels (Red Hat package): до 4.0.0-4.el8ap
python3.12-certifi (Red Hat package): до 2023.5.7-2.el8ap
python3.12-cachetools (Red Hat package): до 5.3.2-2.el8ap
python3.12-brotli (Red Hat package): до 1.2.0-1.el8ap
python3.12-bracex (Red Hat package): до 2.4-2.el8ap
python3.12-botocore (Red Hat package): до 1.34.162-2.el8ap
python3.12-boto3 (Red Hat package): до 1.34.30-2.el8ap
python3.12-black (Red Hat package): до 24.4.2-3.el8ap
python3.12-backoff (Red Hat package): до 2.2.1-2.el8ap
python3.12-azure-core (Red Hat package): до 1.34.0-2.el8ap
python3.12-autobahn (Red Hat package): до 24.4.2-2.el8ap
python3.12-attrs (Red Hat package): до 22.2.0-2.el8ap
python3.12-asyncio-throttle (Red Hat package): до 1.0.2-5.el8ap
python3.12-async-lru (Red Hat package): до 2.0.5-1.el8ap
python3.12-asgiref (Red Hat package): до 3.7.2-2.el8ap
python3.12-argon2-cffi-bindings (Red Hat package): до 21.2.0-2.el8ap
python3.12-argon2-cffi (Red Hat package): до 23.1.0-2.el8ap
python3.12-ansible-sdk (Red Hat package): до 1.0.0-3.el8ap
python3.12-ansible-pylibssh (Red Hat package): до 1.2.2-2.el8ap
python3.12-ansible-compat (Red Hat package): до 25.12.0-3.el8ap
python3.12-aiosignal (Red Hat package): до 1.4.0-1.el8ap
python3.12-aiohttp (Red Hat package): до 3.13.3-2.el8ap
python3.12-aiohappyeyeballs (Red Hat package): до 2.6.1-1.el8ap
python3.12-aiofiles (Red Hat package): до 23.2.1-2.el8ap
python3.12-aiodns (Red Hat package): до 3.2.0-2.el8ap
python3.12-Automat (Red Hat package): до 22.10.0-4.el8ap
pulpcore-selinux (Red Hat package): до 2.0.1-2.el8ap
molecule (Red Hat package): до 25.12.0-2.el8ap
bindep (Red Hat package): до 2.13.0-2.el8ap

automation-hub (Red Hat package): до 4.10.12-1.el8ap
automation-gateway (Red Hat package): до 2.5.20260225-1.el8ap
automation-eda-controller (Red Hat package): до 1.1.16-1.el8ap
automation-controller-fapolicyd (Red Hat package): до 1.0-6.el8ap
automation-controller (Red Hat package): до 4.6.26-1.el8ap
ansible-sign (Red Hat package): до 0.1.4-2.el8ap
ansible-runner (Red Hat package): до 2.4.2-3.el8ap
ansible-rulebook (Red Hat package): до 1.1.7-2.el8ap
ansible-navigator (Red Hat package): до 26.1.1-1.1.el8ap
ansible-lint (Red Hat package): до 26.1.0-3.el8ap
ansible-dev-tools (Red Hat package): до 26.1.0-3.el8ap
ansible-dev-environment (Red Hat package): до 25.12.2-1.2.el8ap
ansible-creator (Red Hat package): до 25.12.0-1.1.el8ap
ansible-core (Red Hat package): до 2.16.16-1.el8ap
ansible-builder (Red Hat package): до 3.1.1-1.2.el8ap
ansible-automation-platform-installer (Red Hat package): до 2.5-21.el8ap
aap-metrics-utility (Red Hat package): до 0.6.0-2.1.el8ap
python3.12-wheel (Red Hat package): до 0.41.2-4.el8_10
python3.12-setuptools (Red Hat package): до 68.2.2-5.el9_6
Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

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: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2026:3959

92

Краткое описание: Отказ в обслуживании в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2026-1285

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: python3.12-django-storages (Red Hat package): до 1.14.2-3.el8ap
python3.12-azure-storage-blob (Red Hat package): до 12.19.0-2.el8ap
yamllint (Red Hat package): до 1.35.1-2.el8ap
uwsgi (Red Hat package): до 2.0.28-2.el8ap
supervisor (Red Hat package): до 4.2.5-2.el8ap
receptor (Red Hat package): до 1.6.3-4.el8ap
python3.12-zope-interface (Red Hat package): до 6.1-2.el8ap
python3.12-zipp (Red Hat package): до 3.19.2-2.el8ap
python3.12-yarl (Red Hat package): до 1.18.3-1.el8ap
python3.12-xxhash (Red Hat package): до 3.4.1-2.el8ap
python3.12-xmlsec (Red Hat package): до 1.3.13-3.el8ap
python3.12-xlwt (Red Hat package): до 1.3.0-5.el8ap
python3.12-xlrd (Red Hat package): до 2.0.1-7.el8ap
python3.12-xds-protos (Red Hat package): до 1.71.2-1.el8ap
python3.12-wrapt (Red Hat package): до 1.16.0-2.el8ap
python3.12-whitenoise (Red Hat package): до 6.6.0-2.el8ap
python3.12-werkzeug (Red Hat package): до 3.0.3-2.el8ap
python3.12-websockets (Red Hat package): до 15.0-3.el8ap
python3.12-websocket-client (Red Hat package): до 1.7.0-3.el8ap
python3.12-wcmatch (Red Hat package): до 8.5-2.el8ap
python3.12-watchdog (Red Hat package): до 5.0.2-2.el8ap
python3.12-virtualenv (Red Hat package): до 20.25.1-2.el8ap
python3.12-validators (Red Hat package): до 0.34.0-2.el8ap
python3.12-uuid6 (Red Hat package): до 2024.1.12-2.el8ap
python3.12-urllib3 (Red Hat package): до 2.6.3-2.el8ap
python3.12-url-normalize (Red Hat package): до 1.4.3-6.el8ap
python3.12-uritemplate (Red Hat package): до 4.1.1-4.el8ap
python3.12-uamqp (Red Hat package): до 1.6.8-2.el8ap
python3.12-typing-extensions (Red Hat package): до 4.15.0-2.el8ap
python3.12-txaio (Red Hat package): до 23.1.1-3.el8ap

python3.12-twisted (Red Hat package): до 24.7.0-2.el8ap
python3.12-tox-ansible (Red Hat package): до 25.12.0-2.el8ap
python3.12-tox (Red Hat package): до 4.15.1-2.el8ap
python3.12-termcolor (Red Hat package): до 3.1.0-2.el8ap
python3.12-tacacs-plus (Red Hat package): до 2.6-3.el8ap
python3.12-tabulate (Red Hat package): до 0.9.0-4.el8ap
python3.12-tablib (Red Hat package): до 3.5.0-2.el8ap
python3.12-subprocess-tee (Red Hat package): до 0.4.2-2.el8ap
python3.12-sqlparse (Red Hat package): до 0.5.3-3.el8ap
python3.12-social-auth-core (Red Hat package): до 4.5.4-2.el8ap
python3.12-social-auth-app-django (Red Hat package): до 5.4.1-2.el8ap
python3.12-smmap (Red Hat package): до 5.0.1-2.el8ap
python3.12-six (Red Hat package): до 1.17.0-1.el8ap
python3.12-service-identity (Red Hat package): до 21.1.0-3.el8ap
python3.12-semantic-version (Red Hat package): до 2.10.0-3.el8ap
python3.12-s3transfer (Red Hat package): до 0.10.0-2.el8ap
python3.12-ruamel-yaml-clib (Red Hat package): до 0.2.15-2.el8ap
python3.12-ruamel-yaml (Red Hat package): до 0.18.15-2.el8ap
python3.12-rsa (Red Hat package): до 4.9-3.el8ap
python3.12-rq-scheduler (Red Hat package): до 0.14.0-1.el8ap
python3.12-rq (Red Hat package): до 2.6.1-1.el8ap
python3.12-rpds-py (Red Hat package): до 0.18.1-3.el8ap
python3.12-rich (Red Hat package): до 13.1.0-2.el8ap
python3.12-rfc3339-validator (Red Hat package): до 0.1.4-2.el8ap
python3.12-resolvelib (Red Hat package): до 1.0.1-2.el8ap
python3.12-requests-oauthlib (Red Hat package): до 1.3.1-2.el8ap
python3.12-requests (Red Hat package): до 2.31.0-4.el8ap
python3.12-referencing (Red Hat package): до 0.36.2-3.el8ap
python3.12-redis (Red Hat package): до 4.6.0-3.el8ap
python3.12-pytz (Red Hat package): до 2024.1-2.el8ap
python3.12-python3-saml (Red Hat package): до 1.16.0-3.el8ap
python3.12-python3-openid (Red Hat package): до 3.2.0-4.el8ap
python3.12-pytest-xdist (Red Hat package): до 3.8.0-2.el8ap
python3.12-pytest-sugar (Red Hat package): до 1.1.1-2.el8ap

python3.12-pytest-plus (Red Hat package): до 0.8.1-2.el8ap
python3.12-pytest-ansible (Red Hat package): до 25.12.0-2.el8ap
python3.12-pytest (Red Hat package): до 9.0.1-2.el8ap
python3.12-pyrad (Red Hat package): до 2.4-3.el8ap
python3.12-pyproject-api (Red Hat package): до 1.6.1-2.el8ap
python3.12-pyparsing (Red Hat package): до 3.1.1-2.el8ap
python3.12-pyjwt (Red Hat package): до 2.7.0-3.el8ap
python3.12-pygtrie (Red Hat package): до 2.5.0-3.el8ap
python3.12-pygments (Red Hat package): до 2.17.2-3.el8ap
python3.12-pyflakes (Red Hat package): до 3.1.0-2.el8ap
python3.12-pydantic (Red Hat package): до 1.10.15-2.el8ap
python3.12-pycodestyle (Red Hat package): до 2.11.1-2.el8ap
python3.12-pycares (Red Hat package): до 4.4.0-3.el8ap
python3.12-pyasn1-modules (Red Hat package): до 0.3.0-2.el8ap
python3.12-pyasn1 (Red Hat package): до 0.5.1-2.el8ap
python3.12-pyOpenSSL (Red Hat package): до 24.1.0-2.el8ap
python3.12-pulpcore (Red Hat package): до 3.49.50-1.el8ap
python3.12-pulp-glue (Red Hat package): до 0.23.2-2.el8ap
python3.12-pulp-container (Red Hat package): до 2.19.3-2.el8ap
python3.12-pulp-ansible (Red Hat package): до 0.25.1-2.el8ap
python3.12-ptyprocess (Red Hat package): до 0.7.0-2.el8ap
python3.12-psycopg (Red Hat package): до 3.2.7-2.el8ap
python3.12-protobuf (Red Hat package): до 5.29.6-1.el8ap
python3.12-propcache (Red Hat package): до 0.4.1-1.el8ap
python3.12-prometheus-client (Red Hat package): до 0.19.0-2.el8ap
python3.12-podman (Red Hat package): до 5.4.0.1-2.el8ap
python3.12-pluggy (Red Hat package): до 1.6.0-2.el8ap
python3.12-platformdirs (Red Hat package): до 4.2.0-2.el8ap
python3.12-pillow (Red Hat package): до 10.3.0-2.el8ap
python3.12-pexpect (Red Hat package): до 4.9.0-2.el8ap
python3.12-persisting-theory (Red Hat package): до 1.0-3.el8ap
python3.12-pbr (Red Hat package): до 6.0.0-3.el8ap
python3.12-pathspec (Red Hat package): до 0.12.1-2.el8ap
python3.12-pathable (Red Hat package): до 0.4.3-2.el8ap

python3.12-parsley (Red Hat package): до 1.3-4.el8ap
python3.12-parse (Red Hat package): до 1.20.1-2.el8ap
python3.12-packaging (Red Hat package): до 23.2-2.el8
python3.12-opentelemetry-contrib (Red Hat package): до 1.28.0-1.el8ap
python3.12-opentelemetry (Red Hat package): до 1.28.0-1.el8ap
python3.12-openpyxl (Red Hat package): до 3.1.2-2.el8ap
python3.12-openapi-spec-validator (Red Hat package): до 0.7.1-2.el8ap
python3.12-openapi-schema-validator (Red Hat package): до 0.6.2-2.el8ap
python3.12-openapi-core (Red Hat package): до 0.19.1-2.el8ap
python3.12-onigurumacffi (Red Hat package): до 1.3.0-2.el8ap
python3.12-odfpy (Red Hat package): до 1.4.1-9.el8ap
python3.12-oauthlib (Red Hat package): до 3.2.2-2.el8ap
python3.12-nh3 (Red Hat package): до 0.2.18-2.el8ap
python3.12-netaddr (Red Hat package): до 1.2.1-2.el8ap
python3.12-mypy-extensions (Red Hat package): до 1.0.0-2.el8ap
python3.12-multidict (Red Hat package): до 6.0.4-2.el8ap
python3.12-more-itertools (Red Hat package): до 10.2.0-2.el8ap
python3.12-mccabe (Red Hat package): до 0.7.0-3.el8ap
python3.12-marshmallow (Red Hat package): до 3.26.2-1.el8ap
python3.12-markupsafe (Red Hat package): до 2.1.5-2.el8ap
python3.12-markuppy (Red Hat package): до 1.14-5.el8ap
python3.12-markdown (Red Hat package): до 3.5.2-2.el8ap
python3.12-lxml (Red Hat package): до 5.3.0-2.el8ap
python3.12-lockfile (Red Hat package): до 0.12.2-3.el8ap
python3.12-ldap-filter (Red Hat package): до 1.0.1-2.el8ap
python3.12-ldap (Red Hat package): до 3.4.5-1.el8ap
python3.12-lazy-object-proxy (Red Hat package): до 1.10.0-2.el8ap
python3.12-kubernetes (Red Hat package): до 26.1.0-3.el8ap
python3.12-jwcrypto (Red Hat package): до 1.5.6-2.el8ap
python3.12-jsonschema-specifications (Red Hat package): до 2023.12.1-2.el8ap
python3.12-jsonschema-path (Red Hat package): до 0.3.4-2.el8ap
python3.12-jsonschema (Red Hat package): до 4.21.1-2.el8ap
python3.12-json-stream-rs-tokenizer (Red Hat package): до 0.4.26-2.el8ap
python3.12-json-stream (Red Hat package): до 2.3.2-2.el8ap

python3.12-jq (Red Hat package): до 1.6.0-2.el8ap
python3.12-jpy (Red Hat package): до 0.15.0-2.el8ap
python3.12-jmespath (Red Hat package): до 1.0.1-3.el8ap
python3.12-jinja2 (Red Hat package): до 3.1.6-2.el8ap
python3.12-janus (Red Hat package): до 1.0.0-3.el8ap
python3.12-isodate (Red Hat package): до 0.6.1-3.el8ap
python3.12-insights-analytics-collector (Red Hat package): до 0.3.2-3.el8ap
python3.12-iniconfig (Red Hat package): до 2.0.0-2.el8ap
python3.12-inflection (Red Hat package): до 0.5.1-5.el8ap
python3.12-incremental (Red Hat package): до 24.7.2-2.el8ap
python3.12-importlib-metadata (Red Hat package): до 6.0.1-3.el8ap
python3.12-hyperlink (Red Hat package): до 21.0.0-3.el8ap
python3.12-gunicorn (Red Hat package): до 23.0.0-2.el8ap
python3.12-grpcio (Red Hat package): до 1.71.2-1.el8ap
python3.12-googleapis-common-protos (Red Hat package): до 1.72.0-1.el8ap
python3.12-google-auth (Red Hat package): до 2.27.0-2.el8ap
python3.12-gnupg (Red Hat package): до 0.5.2-2.el8ap
python3.12-gitpython (Red Hat package): до 3.1.41-2.el8ap
python3.12-gitdb (Red Hat package): до 4.0.11-2.el8ap
python3.12-galaxy-ng (Red Hat package): до 4.10.12-1.el8ap
python3.12-galaxy-importer (Red Hat package): до 0.4.37-3.el8ap
python3.12-frozenlist (Red Hat package): до 1.4.0-2.el8ap
python3.12-freezegun (Red Hat package): до 1.5.5-1.el8ap
python3.12-flake8 (Red Hat package): до 6.1.0-3.el8ap
python3.12-filelock (Red Hat package): до 3.13.1-2.el8ap
python3.12-execnet (Red Hat package): до 2.1.2-2.el8ap
python3.12-et-xmlfile (Red Hat package): до 1.1.0-4.el8ap
python3.12-enrich (Red Hat package): до 1.2.7-3.el8ap
python3.12-ecdsa (Red Hat package): до 0.18.0-2.el8ap
python3.12-dynaconf (Red Hat package): до 3.2.11-2.el8ap
python3.12-drools-jpy (Red Hat package): до 0.3.10-2.el8ap
python3.12-drf-spectacular (Red Hat package): до 0.26.5-3.el8ap
python3.12-drf-nested-routers (Red Hat package): до 0.93.5-2.el8ap
python3.12-drf-access-policy (Red Hat package): до 1.5.0-2.el8ap

python3.12-dpath (Red Hat package): до 2.1.6-2.el8ap
python3.12-djangorestframework-queryfields (Red Hat package): до 1.1.0-2.el8ap
python3.12-djangorestframework (Red Hat package): до 3.15.1-2.el8ap
python3.12-django-split-settings (Red Hat package): до 1.2.0-3.el8ap
python3.12-django-rq (Red Hat package): до 3.2.2-1.el8ap
python3.12-django-redis (Red Hat package): до 5.4.0-2.el8ap
python3.12-django-prometheus (Red Hat package): до 2.3.1-3.el8ap
python3.12-django-picklefield (Red Hat package): до 3.1-2.el8ap
python3.12-django-oauth-toolkit (Red Hat package): до 2.3.0-2.el8ap
python3.12-django-lifecycle (Red Hat package): до 1.1.2-2.el8ap
python3.12-django-ipware (Red Hat package): до 3.0.7-4.el8ap
python3.12-django-import-export (Red Hat package): до 3.3.6-3.el8ap
python3.12-django-guid (Red Hat package): до 3.4.0-2.el8ap
python3.12-django-flags (Red Hat package): до 5.0.13-2.el8ap
python3.12-django-filter (Red Hat package): до 23.5-2.el8ap
python3.12-django-extensions (Red Hat package): до 4.1-2.el8ap
python3.12-django-dynamic-preferences (Red Hat package): до 1.16.0-2.el8ap
python3.12-django-crum (Red Hat package): до 0.7.9-3.el8ap
python3.12-django-auth-ldap (Red Hat package): до 4.0.0-3.el8ap
python3.12-django-ansible-base (Red Hat package): до 2.5.20260225-1.el8ap
python3.12-django (Red Hat package): до 4.2.28-1.el8ap
python3.12-distro (Red Hat package): до 1.9.0-2.el8ap
python3.12-distlib (Red Hat package): до 0.4.0-2.el8ap
python3.12-dispatcherd (Red Hat package): до 2025.5.19-3.el8ap
python3.12-diff-match-patch (Red Hat package): до 20230430-2.el8ap
python3.12-deprecated (Red Hat package): до 1.2.14-2.el8ap
python3.12-defusedxml (Red Hat package): до 0.7.1-5.el8ap
python3.12-dateutil (Red Hat package): до 2.8.2-3.el8ap
python3.12-daphne (Red Hat package): до 4.0.0-4.el8ap
python3.12-daemon (Red Hat package): до 3.1.2-3.el8ap
python3.12-cryptography (Red Hat package): до 42.0.5-2.el8ap
python3.12-crontab (Red Hat package): до 1.0.5-1.el8ap
python3.12-croniter (Red Hat package): до 2.0.1-2.el8ap
python3.12-constantly (Red Hat package): до 23.10.4-1.el8ap

python3.12-commonmark (Red Hat package): до 0.9.1-7.el8ap
python3.12-colorama (Red Hat package): до 0.4.6-2.el8ap
python3.12-click-help-colors (Red Hat package): до 0.9.4-2.el8ap
python3.12-click (Red Hat package): до 8.1.7-2.el8ap
python3.12-chardet (Red Hat package): до 5.2.0-3.el8ap
python3.12-channels (Red Hat package): до 4.0.0-4.el8ap
python3.12-certifi (Red Hat package): до 2023.5.7-2.el8ap
python3.12-cachetools (Red Hat package): до 5.3.2-2.el8ap
python3.12-brotli (Red Hat package): до 1.2.0-1.el8ap
python3.12-bracex (Red Hat package): до 2.4-2.el8ap
python3.12-botocore (Red Hat package): до 1.34.162-2.el8ap
python3.12-boto3 (Red Hat package): до 1.34.30-2.el8ap
python3.12-black (Red Hat package): до 24.4.2-3.el8ap
python3.12-backoff (Red Hat package): до 2.2.1-2.el8ap
python3.12-azure-core (Red Hat package): до 1.34.0-2.el8ap
python3.12-autobahn (Red Hat package): до 24.4.2-2.el8ap
python3.12-attrs (Red Hat package): до 22.2.0-2.el8ap
python3.12-asyncio-throttle (Red Hat package): до 1.0.2-5.el8ap
python3.12-async-lru (Red Hat package): до 2.0.5-1.el8ap
python3.12-asgiref (Red Hat package): до 3.7.2-2.el8ap
python3.12-argon2-cffi-bindings (Red Hat package): до 21.2.0-2.el8ap
python3.12-argon2-cffi (Red Hat package): до 23.1.0-2.el8ap
python3.12-ansible-sdk (Red Hat package): до 1.0.0-3.el8ap
python3.12-ansible-pylibssh (Red Hat package): до 1.2.2-2.el8ap
python3.12-ansible-compat (Red Hat package): до 25.12.0-3.el8ap
python3.12-aiosignal (Red Hat package): до 1.4.0-1.el8ap
python3.12-aiohttp (Red Hat package): до 3.13.3-2.el8ap
python3.12-aiohappyeyeballs (Red Hat package): до 2.6.1-1.el8ap
python3.12-aiofiles (Red Hat package): до 23.2.1-2.el8ap
python3.12-aiodns (Red Hat package): до 3.2.0-2.el8ap
python3.12-Automat (Red Hat package): до 22.10.0-4.el8ap
pulpcore-selinux (Red Hat package): до 2.0.1-2.el8ap
molecule (Red Hat package): до 25.12.0-2.el8ap
bindep (Red Hat package): до 2.13.0-2.el8ap

automation-hub (Red Hat package): до 4.10.12-1.el8ap
automation-gateway (Red Hat package): до 2.5.20260225-1.el8ap
automation-eda-controller (Red Hat package): до 1.1.16-1.el8ap
automation-controller-fapolicyd (Red Hat package): до 1.0-6.el8ap
automation-controller (Red Hat package): до 4.6.26-1.el8ap
ansible-sign (Red Hat package): до 0.1.4-2.el8ap
ansible-runner (Red Hat package): до 2.4.2-3.el8ap
ansible-rulebook (Red Hat package): до 1.1.7-2.el8ap
ansible-navigator (Red Hat package): до 26.1.1-1.1.el8ap
ansible-lint (Red Hat package): до 26.1.0-3.el8ap
ansible-dev-tools (Red Hat package): до 26.1.0-3.el8ap
ansible-dev-environment (Red Hat package): до 25.12.2-1.2.el8ap
ansible-creator (Red Hat package): до 25.12.0-1.1.el8ap
ansible-core (Red Hat package): до 2.16.16-1.el8ap
ansible-builder (Red Hat package): до 3.1.1-1.2.el8ap
ansible-automation-platform-installer (Red Hat package): до 2.5-21.el8ap
aap-metrics-utility (Red Hat package): до 0.6.0-2.1.el8ap
python3.12-wheel (Red Hat package): до 0.41.2-4.el8_10
python3.12-setuptools (Red Hat package): до 68.2.2-5.el9_6
Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

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: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2026:3959

93

Краткое описание: Отказ в обслуживании в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-69223

Идентификатор программной ошибки: CWE-409 Некорректная обработка данных с высокой степенью сжатия (увеличение объема данных)

Уязвимый продукт: python3.12-django-storages (Red Hat package): до 1.14.2-3.el8ap
python3.12-azure-storage-blob (Red Hat package): до 12.19.0-2.el8ap
yamllint (Red Hat package): до 1.35.1-2.el8ap
uwsgi (Red Hat package): до 2.0.28-2.el8ap
supervisor (Red Hat package): до 4.2.5-2.el8ap
receptor (Red Hat package): до 1.6.3-4.el8ap
python3.12-zope-interface (Red Hat package): до 6.1-2.el8ap
python3.12-zipp (Red Hat package): до 3.19.2-2.el8ap
python3.12-yarl (Red Hat package): до 1.18.3-1.el8ap
python3.12-xxhash (Red Hat package): до 3.4.1-2.el8ap
python3.12-xmlsec (Red Hat package): до 1.3.13-3.el8ap
python3.12-xlwt (Red Hat package): до 1.3.0-5.el8ap
python3.12-xlrd (Red Hat package): до 2.0.1-7.el8ap
python3.12-xds-protos (Red Hat package): до 1.71.2-1.el8ap
python3.12-wrapt (Red Hat package): до 1.16.0-2.el8ap
python3.12-whitenoise (Red Hat package): до 6.6.0-2.el8ap
python3.12-werkzeug (Red Hat package): до 3.0.3-2.el8ap
python3.12-websockets (Red Hat package): до 15.0-3.el8ap
python3.12-websocket-client (Red Hat package): до 1.7.0-3.el8ap
python3.12-wcmatch (Red Hat package): до 8.5-2.el8ap
python3.12-watchdog (Red Hat package): до 5.0.2-2.el8ap
python3.12-virtualenv (Red Hat package): до 20.25.1-2.el8ap
python3.12-validators (Red Hat package): до 0.34.0-2.el8ap
python3.12-uuid6 (Red Hat package): до 2024.1.12-2.el8ap
python3.12-urllib3 (Red Hat package): до 2.6.3-2.el8ap
python3.12-url-normalize (Red Hat package): до 1.4.3-6.el8ap
python3.12-uritemplate (Red Hat package): до 4.1.1-4.el8ap
python3.12-uamqp (Red Hat package): до 1.6.8-2.el8ap
python3.12-typing-extensions (Red Hat package): до 4.15.0-2.el8ap

python3.12-txaio (Red Hat package): до 23.1.1-3.el8ap
python3.12-twisted (Red Hat package): до 24.7.0-2.el8ap
python3.12-tox-ansible (Red Hat package): до 25.12.0-2.el8ap
python3.12-tox (Red Hat package): до 4.15.1-2.el8ap
python3.12-termcolor (Red Hat package): до 3.1.0-2.el8ap
python3.12-tacacs-plus (Red Hat package): до 2.6-3.el8ap
python3.12-tabulate (Red Hat package): до 0.9.0-4.el8ap
python3.12-tablib (Red Hat package): до 3.5.0-2.el8ap
python3.12-subprocess-tee (Red Hat package): до 0.4.2-2.el8ap
python3.12-sqlparse (Red Hat package): до 0.5.3-3.el8ap
python3.12-social-auth-core (Red Hat package): до 4.5.4-2.el8ap
python3.12-social-auth-app-django (Red Hat package): до 5.4.1-2.el8ap
python3.12-smmap (Red Hat package): до 5.0.1-2.el8ap
python3.12-six (Red Hat package): до 1.17.0-1.el8ap
python3.12-service-identity (Red Hat package): до 21.1.0-3.el8ap
python3.12-semantic-version (Red Hat package): до 2.10.0-3.el8ap
python3.12-s3transfer (Red Hat package): до 0.10.0-2.el8ap
python3.12-ruamel-yaml-clib (Red Hat package): до 0.2.15-2.el8ap
python3.12-ruamel-yaml (Red Hat package): до 0.18.15-2.el8ap
python3.12-rsa (Red Hat package): до 4.9-3.el8ap
python3.12-rq-scheduler (Red Hat package): до 0.14.0-1.el8ap
python3.12-rq (Red Hat package): до 2.6.1-1.el8ap
python3.12-rpds-py (Red Hat package): до 0.18.1-3.el8ap
python3.12-rich (Red Hat package): до 13.1.0-2.el8ap
python3.12-rfc3339-validator (Red Hat package): до 0.1.4-2.el8ap
python3.12-resolvelib (Red Hat package): до 1.0.1-2.el8ap
python3.12-requests-oauthlib (Red Hat package): до 1.3.1-2.el8ap
python3.12-requests (Red Hat package): до 2.31.0-4.el8ap
python3.12-referencing (Red Hat package): до 0.36.2-3.el8ap
python3.12-redis (Red Hat package): до 4.6.0-3.el8ap
python3.12-pytz (Red Hat package): до 2024.1-2.el8ap
python3.12-python3-saml (Red Hat package): до 1.16.0-3.el8ap
python3.12-python3-openid (Red Hat package): до 3.2.0-4.el8ap
python3.12-pytest-xdist (Red Hat package): до 3.8.0-2.el8ap

python3.12-pytest-sugar (Red Hat package): до 1.1.1-2.el8ap
python3.12-pytest-plus (Red Hat package): до 0.8.1-2.el8ap
python3.12-pytest-ansible (Red Hat package): до 25.12.0-2.el8ap
python3.12-pytest (Red Hat package): до 9.0.1-2.el8ap
python3.12-pyrad (Red Hat package): до 2.4-3.el8ap
python3.12-pyproject-api (Red Hat package): до 1.6.1-2.el8ap
python3.12-pyparsing (Red Hat package): до 3.1.1-2.el8ap
python3.12-pyjwt (Red Hat package): до 2.7.0-3.el8ap
python3.12-pygtrie (Red Hat package): до 2.5.0-3.el8ap
python3.12-pygments (Red Hat package): до 2.17.2-3.el8ap
python3.12-pyflakes (Red Hat package): до 3.1.0-2.el8ap
python3.12-pydantic (Red Hat package): до 1.10.15-2.el8ap
python3.12-pycodestyle (Red Hat package): до 2.11.1-2.el8ap
python3.12-pycares (Red Hat package): до 4.4.0-3.el8ap
python3.12-pyasn1-modules (Red Hat package): до 0.3.0-2.el8ap
python3.12-pyasn1 (Red Hat package): до 0.5.1-2.el8ap
python3.12-pyOpenSSL (Red Hat package): до 24.1.0-2.el8ap
python3.12-pulpcore (Red Hat package): до 3.49.50-1.el8ap
python3.12-pulp-glue (Red Hat package): до 0.23.2-2.el8ap
python3.12-pulp-container (Red Hat package): до 2.19.3-2.el8ap
python3.12-pulp-ansible (Red Hat package): до 0.25.1-2.el8ap
python3.12-ptyprocess (Red Hat package): до 0.7.0-2.el8ap
python3.12-psycopg (Red Hat package): до 3.2.7-2.el8ap
python3.12-protobuf (Red Hat package): до 5.29.6-1.el8ap
python3.12-propcache (Red Hat package): до 0.4.1-1.el8ap
python3.12-prometheus-client (Red Hat package): до 0.19.0-2.el8ap
python3.12-podman (Red Hat package): до 5.4.0.1-2.el8ap
python3.12-pluggy (Red Hat package): до 1.6.0-2.el8ap
python3.12-platformdirs (Red Hat package): до 4.2.0-2.el8ap
python3.12-pillow (Red Hat package): до 10.3.0-2.el8ap
python3.12-pexpect (Red Hat package): до 4.9.0-2.el8ap
python3.12-persisting-theory (Red Hat package): до 1.0-3.el8ap
python3.12-pbr (Red Hat package): до 6.0.0-3.el8ap
python3.12-pathspec (Red Hat package): до 0.12.1-2.el8ap

python3.12-pathable (Red Hat package): до 0.4.3-2.el8ap
python3.12-parsley (Red Hat package): до 1.3-4.el8ap
python3.12-parse (Red Hat package): до 1.20.1-2.el8ap
python3.12-packaging (Red Hat package): до 23.2-2.el8
python3.12-opentelemetry-contrib (Red Hat package): до 1.28.0-1.el8ap
python3.12-opentelemetry (Red Hat package): до 1.28.0-1.el8ap
python3.12-openpyxl (Red Hat package): до 3.1.2-2.el8ap
python3.12-openapi-spec-validator (Red Hat package): до 0.7.1-2.el8ap
python3.12-openapi-schema-validator (Red Hat package): до 0.6.2-2.el8ap
python3.12-openapi-core (Red Hat package): до 0.19.1-2.el8ap
python3.12-onigurumacffi (Red Hat package): до 1.3.0-2.el8ap
python3.12-odfpy (Red Hat package): до 1.4.1-9.el8ap
python3.12-oauthlib (Red Hat package): до 3.2.2-2.el8ap
python3.12-nh3 (Red Hat package): до 0.2.18-2.el8ap
python3.12-netaddr (Red Hat package): до 1.2.1-2.el8ap
python3.12-mypy-extensions (Red Hat package): до 1.0.0-2.el8ap
python3.12-multidict (Red Hat package): до 6.0.4-2.el8ap
python3.12-more-itertools (Red Hat package): до 10.2.0-2.el8ap
python3.12-mccabe (Red Hat package): до 0.7.0-3.el8ap
python3.12-marshmallow (Red Hat package): до 3.26.2-1.el8ap
python3.12-markupsafe (Red Hat package): до 2.1.5-2.el8ap
python3.12-markuppy (Red Hat package): до 1.14-5.el8ap
python3.12-markdown (Red Hat package): до 3.5.2-2.el8ap
python3.12-lxml (Red Hat package): до 5.3.0-2.el8ap
python3.12-lockfile (Red Hat package): до 0.12.2-3.el8ap
python3.12-ldap-filter (Red Hat package): до 1.0.1-2.el8ap
python3.12-ldap (Red Hat package): до 3.4.5-1.el8ap
python3.12-lazy-object-proxy (Red Hat package): до 1.10.0-2.el8ap
python3.12-kubernetes (Red Hat package): до 26.1.0-3.el8ap
python3.12-jwcrypto (Red Hat package): до 1.5.6-2.el8ap
python3.12-jsonschema-specifications (Red Hat package): до 2023.12.1-2.el8ap
python3.12-jsonschema-path (Red Hat package): до 0.3.4-2.el8ap
python3.12-jsonschema (Red Hat package): до 4.21.1-2.el8ap
python3.12-json-stream-rs-tokenizer (Red Hat package): до 0.4.26-2.el8ap

python3.12-json-stream (Red Hat package): до 2.3.2-2.el8ap
python3.12-jq (Red Hat package): до 1.6.0-2.el8ap
python3.12-jpy (Red Hat package): до 0.15.0-2.el8ap
python3.12-jmespath (Red Hat package): до 1.0.1-3.el8ap
python3.12-jinja2 (Red Hat package): до 3.1.6-2.el8ap
python3.12-janus (Red Hat package): до 1.0.0-3.el8ap
python3.12-isodate (Red Hat package): до 0.6.1-3.el8ap
python3.12-insights-analytics-collector (Red Hat package): до 0.3.2-3.el8ap
python3.12-iniconfig (Red Hat package): до 2.0.0-2.el8ap
python3.12-inflection (Red Hat package): до 0.5.1-5.el8ap
python3.12-incremental (Red Hat package): до 24.7.2-2.el8ap
python3.12-importlib-metadata (Red Hat package): до 6.0.1-3.el8ap
python3.12-hyperlink (Red Hat package): до 21.0.0-3.el8ap
python3.12-gunicorn (Red Hat package): до 23.0.0-2.el8ap
python3.12-grpcio (Red Hat package): до 1.71.2-1.el8ap
python3.12-googleapis-common-protos (Red Hat package): до 1.72.0-1.el8ap
python3.12-google-auth (Red Hat package): до 2.27.0-2.el8ap
python3.12-gnupg (Red Hat package): до 0.5.2-2.el8ap
python3.12-gitpython (Red Hat package): до 3.1.41-2.el8ap
python3.12-gitdb (Red Hat package): до 4.0.11-2.el8ap
python3.12-galaxy-ng (Red Hat package): до 4.10.12-1.el8ap
python3.12-galaxy-importer (Red Hat package): до 0.4.37-3.el8ap
python3.12-frozenlist (Red Hat package): до 1.4.0-2.el8ap
python3.12-freezegun (Red Hat package): до 1.5.5-1.el8ap
python3.12-flake8 (Red Hat package): до 6.1.0-3.el8ap
python3.12-filelock (Red Hat package): до 3.13.1-2.el8ap
python3.12-execnet (Red Hat package): до 2.1.2-2.el8ap
python3.12-et-xmlfile (Red Hat package): до 1.1.0-4.el8ap
python3.12-enrich (Red Hat package): до 1.2.7-3.el8ap
python3.12-ecdsa (Red Hat package): до 0.18.0-2.el8ap
python3.12-dynaconf (Red Hat package): до 3.2.11-2.el8ap
python3.12-drools-jpy (Red Hat package): до 0.3.10-2.el8ap
python3.12-drf-spectacular (Red Hat package): до 0.26.5-3.el8ap
python3.12-drf-nested-routers (Red Hat package): до 0.93.5-2.el8ap

python3.12-drf-access-policy (Red Hat package): до 1.5.0-2.el8ap
python3.12-dpath (Red Hat package): до 2.1.6-2.el8ap
python3.12-djangorestframework-queryfields (Red Hat package): до 1.1.0-2.el8ap
python3.12-djangorestframework (Red Hat package): до 3.15.1-2.el8ap
python3.12-django-split-settings (Red Hat package): до 1.2.0-3.el8ap
python3.12-django-rq (Red Hat package): до 3.2.2-1.el8ap
python3.12-django-redis (Red Hat package): до 5.4.0-2.el8ap
python3.12-django-prometheus (Red Hat package): до 2.3.1-3.el8ap
python3.12-django-picklefield (Red Hat package): до 3.1-2.el8ap
python3.12-django-oauth-toolkit (Red Hat package): до 2.3.0-2.el8ap
python3.12-django-lifecycle (Red Hat package): до 1.1.2-2.el8ap
python3.12-django-ipware (Red Hat package): до 3.0.7-4.el8ap
python3.12-django-import-export (Red Hat package): до 3.3.6-3.el8ap
python3.12-django-guid (Red Hat package): до 3.4.0-2.el8ap
python3.12-django-flags (Red Hat package): до 5.0.13-2.el8ap
python3.12-django-filter (Red Hat package): до 23.5-2.el8ap
python3.12-django-extensions (Red Hat package): до 4.1-2.el8ap
python3.12-django-dynamic-preferences (Red Hat package): до 1.16.0-2.el8ap
python3.12-django-crum (Red Hat package): до 0.7.9-3.el8ap
python3.12-django-auth-ldap (Red Hat package): до 4.0.0-3.el8ap
python3.12-django-ansible-base (Red Hat package): до 2.5.20260225-1.el8ap
python3.12-django (Red Hat package): до 4.2.28-1.el8ap
python3.12-distro (Red Hat package): до 1.9.0-2.el8ap
python3.12-distlib (Red Hat package): до 0.4.0-2.el8ap
python3.12-dispatcherd (Red Hat package): до 2025.5.19-3.el8ap
python3.12-diff-match-patch (Red Hat package): до 20230430-2.el8ap
python3.12-deprecated (Red Hat package): до 1.2.14-2.el8ap
python3.12-defusedxml (Red Hat package): до 0.7.1-5.el8ap
python3.12-dateutil (Red Hat package): до 2.8.2-3.el8ap
python3.12-daphne (Red Hat package): до 4.0.0-4.el8ap
python3.12-daemon (Red Hat package): до 3.1.2-3.el8ap
python3.12-cryptography (Red Hat package): до 42.0.5-2.el8ap
python3.12-crontab (Red Hat package): до 1.0.5-1.el8ap
python3.12-croniter (Red Hat package): до 2.0.1-2.el8ap

python3.12-constantly (Red Hat package): до 23.10.4-1.el8ap
python3.12-commonmark (Red Hat package): до 0.9.1-7.el8ap
python3.12-colorama (Red Hat package): до 0.4.6-2.el8ap
python3.12-click-help-colors (Red Hat package): до 0.9.4-2.el8ap
python3.12-click (Red Hat package): до 8.1.7-2.el8ap
python3.12-chardet (Red Hat package): до 5.2.0-3.el8ap
python3.12-channels (Red Hat package): до 4.0.0-4.el8ap
python3.12-certifi (Red Hat package): до 2023.5.7-2.el8ap
python3.12-cachetools (Red Hat package): до 5.3.2-2.el8ap
python3.12-brotli (Red Hat package): до 1.2.0-1.el8ap
python3.12-bracex (Red Hat package): до 2.4-2.el8ap
python3.12-botocore (Red Hat package): до 1.34.162-2.el8ap
python3.12-boto3 (Red Hat package): до 1.34.30-2.el8ap
python3.12-black (Red Hat package): до 24.4.2-3.el8ap
python3.12-backoff (Red Hat package): до 2.2.1-2.el8ap
python3.12-azure-core (Red Hat package): до 1.34.0-2.el8ap
python3.12-autobahn (Red Hat package): до 24.4.2-2.el8ap
python3.12-attrs (Red Hat package): до 22.2.0-2.el8ap
python3.12-asyncio-throttle (Red Hat package): до 1.0.2-5.el8ap
python3.12-async-lru (Red Hat package): до 2.0.5-1.el8ap
python3.12-asgiref (Red Hat package): до 3.7.2-2.el8ap
python3.12-argon2-cffi-bindings (Red Hat package): до 21.2.0-2.el8ap
python3.12-argon2-cffi (Red Hat package): до 23.1.0-2.el8ap
python3.12-ansible-sdk (Red Hat package): до 1.0.0-3.el8ap
python3.12-ansible-pylibssh (Red Hat package): до 1.2.2-2.el8ap
python3.12-ansible-compat (Red Hat package): до 25.12.0-3.el8ap
python3.12-aiosignal (Red Hat package): до 1.4.0-1.el8ap
python3.12-aiohttp (Red Hat package): до 3.13.3-2.el8ap
python3.12-aiohappyeyeballs (Red Hat package): до 2.6.1-1.el8ap
python3.12-aiofiles (Red Hat package): до 23.2.1-2.el8ap
python3.12-aiodns (Red Hat package): до 3.2.0-2.el8ap
python3.12-Automat (Red Hat package): до 22.10.0-4.el8ap
pulpcore-selinux (Red Hat package): до 2.0.1-2.el8ap
molecule (Red Hat package): до 25.12.0-2.el8ap

bindep (Red Hat package): до 2.13.0-2.el8ap
automation-hub (Red Hat package): до 4.10.12-1.el8ap
automation-gateway (Red Hat package): до 2.5.20260225-1.el8ap
automation-eda-controller (Red Hat package): до 1.1.16-1.el8ap
automation-controller-fapolicyd (Red Hat package): до 1.0-6.el8ap
automation-controller (Red Hat package): до 4.6.26-1.el8ap
ansible-sign (Red Hat package): до 0.1.4-2.el8ap
ansible-runner (Red Hat package): до 2.4.2-3.el8ap
ansible-rulebook (Red Hat package): до 1.1.7-2.el8ap
ansible-navigator (Red Hat package): до 26.1.1-1.1.el8ap
ansible-lint (Red Hat package): до 26.1.0-3.el8ap
ansible-dev-tools (Red Hat package): до 26.1.0-3.el8ap
ansible-dev-environment (Red Hat package): до 25.12.2-1.2.el8ap
ansible-creator (Red Hat package): до 25.12.0-1.1.el8ap
ansible-core (Red Hat package): до 2.16.16-1.el8ap
ansible-builder (Red Hat package): до 3.1.1-1.2.el8ap
ansible-automation-platform-installer (Red Hat package): до 2.5-21.el8ap
aap-metrics-utility (Red Hat package): до 0.6.0-2.1.el8ap
python3.12-wheel (Red Hat package): до 0.41.2-4.el8_10
python3.12-setuptools (Red Hat package): до 68.2.2-5.el9_6
Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного HTTP-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: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2026:3959

94	**Краткое описание:** Межсайтовый скриптинг в Ansible Automation Platform 2.5 packages **Идентификатор уязвимости:** CVE-2026-22029 **Идентификатор программной ошибки:** CWE-79 Некорректная нейтрализация входных данных при генерировании веб-страниц (межсайтовое выполнение сценариев) **Уязвимый продукт:** python3.12-django-storages (Red Hat package): до 1.14.2-3.el8ap python3.12-azure-storage-blob (Red Hat package): до 12.19.0-2.el8ap yamllint (Red Hat package): до 1.35.1-2.el8ap uwsgi (Red Hat package): до 2.0.28-2.el8ap supervisor (Red Hat package): до 4.2.5-2.el8ap receptor (Red Hat package): до 1.6.3-4.el8ap python3.12-zope-interface (Red Hat package): до 6.1-2.el8ap python3.12-zipp (Red Hat package): до 3.19.2-2.el8ap python3.12-yarl (Red Hat package): до 1.18.3-1.el8ap python3.12-xxhash (Red Hat package): до 3.4.1-2.el8ap python3.12-xmlsec (Red Hat package): до 1.3.13-3.el8ap python3.12-xlwt (Red Hat package): до 1.3.0-5.el8ap python3.12-xlrd (Red Hat package): до 2.0.1-7.el8ap python3.12-xds-protos (Red Hat package): до 1.71.2-1.el8ap python3.12-wrapt (Red Hat package): до 1.16.0-2.el8ap python3.12-whitenoise (Red Hat package): до 6.6.0-2.el8ap python3.12-werkzeug (Red Hat package): до 3.0.3-2.el8ap python3.12-websockets (Red Hat package): до 15.0-3.el8ap python3.12-websocket-client (Red Hat package): до 1.7.0-3.el8ap python3.12-wcmatch (Red Hat package): до 8.5-2.el8ap python3.12-watchdog (Red Hat package): до 5.0.2-2.el8ap python3.12-virtualenv (Red Hat package): до 20.25.1-2.el8ap python3.12-validators (Red Hat package): до 0.34.0-2.el8ap python3.12-uuid6 (Red Hat package): до 2024.1.12-2.el8ap python3.12-urllib3 (Red Hat package): до 2.6.3-2.el8ap python3.12-url-normalize (Red Hat package): до 1.4.3-6.el8ap python3.12-uritemplate (Red Hat package): до 4.1.1-4.el8ap python3.12-uamqp (Red Hat package): до 1.6.8-2.el8ap python3.12-typing-extensions (Red Hat package): до 4.15.0-2.el8ap

python3.12-txaio (Red Hat package): до 23.1.1-3.el8ap
python3.12-twisted (Red Hat package): до 24.7.0-2.el8ap
python3.12-tox-ansible (Red Hat package): до 25.12.0-2.el8ap
python3.12-tox (Red Hat package): до 4.15.1-2.el8ap
python3.12-termcolor (Red Hat package): до 3.1.0-2.el8ap
python3.12-tacacs-plus (Red Hat package): до 2.6-3.el8ap
python3.12-tabulate (Red Hat package): до 0.9.0-4.el8ap
python3.12-tablib (Red Hat package): до 3.5.0-2.el8ap
python3.12-subprocess-tee (Red Hat package): до 0.4.2-2.el8ap
python3.12-sqlparse (Red Hat package): до 0.5.3-3.el8ap
python3.12-social-auth-core (Red Hat package): до 4.5.4-2.el8ap
python3.12-social-auth-app-django (Red Hat package): до 5.4.1-2.el8ap
python3.12-smmap (Red Hat package): до 5.0.1-2.el8ap
python3.12-six (Red Hat package): до 1.17.0-1.el8ap
python3.12-service-identity (Red Hat package): до 21.1.0-3.el8ap
python3.12-semantic-version (Red Hat package): до 2.10.0-3.el8ap
python3.12-s3transfer (Red Hat package): до 0.10.0-2.el8ap
python3.12-ruamel-yaml-clib (Red Hat package): до 0.2.15-2.el8ap
python3.12-ruamel-yaml (Red Hat package): до 0.18.15-2.el8ap
python3.12-rsa (Red Hat package): до 4.9-3.el8ap
python3.12-rq-scheduler (Red Hat package): до 0.14.0-1.el8ap
python3.12-rq (Red Hat package): до 2.6.1-1.el8ap
python3.12-rpds-py (Red Hat package): до 0.18.1-3.el8ap
python3.12-rich (Red Hat package): до 13.1.0-2.el8ap
python3.12-rfc3339-validator (Red Hat package): до 0.1.4-2.el8ap
python3.12-resolvelib (Red Hat package): до 1.0.1-2.el8ap
python3.12-requests-oauthlib (Red Hat package): до 1.3.1-2.el8ap
python3.12-requests (Red Hat package): до 2.31.0-4.el8ap
python3.12-referencing (Red Hat package): до 0.36.2-3.el8ap
python3.12-redis (Red Hat package): до 4.6.0-3.el8ap
python3.12-pytz (Red Hat package): до 2024.1-2.el8ap
python3.12-python3-saml (Red Hat package): до 1.16.0-3.el8ap
python3.12-python3-openid (Red Hat package): до 3.2.0-4.el8ap
python3.12-pytest-xdist (Red Hat package): до 3.8.0-2.el8ap

python3.12-pytest-sugar (Red Hat package): до 1.1.1-2.el8ap
python3.12-pytest-plus (Red Hat package): до 0.8.1-2.el8ap
python3.12-pytest-ansible (Red Hat package): до 25.12.0-2.el8ap
python3.12-pytest (Red Hat package): до 9.0.1-2.el8ap
python3.12-pyrad (Red Hat package): до 2.4-3.el8ap
python3.12-pyproject-api (Red Hat package): до 1.6.1-2.el8ap
python3.12-pyparsing (Red Hat package): до 3.1.1-2.el8ap
python3.12-pyjwt (Red Hat package): до 2.7.0-3.el8ap
python3.12-pygtrie (Red Hat package): до 2.5.0-3.el8ap
python3.12-pygments (Red Hat package): до 2.17.2-3.el8ap
python3.12-pyflakes (Red Hat package): до 3.1.0-2.el8ap
python3.12-pydantic (Red Hat package): до 1.10.15-2.el8ap
python3.12-pycodestyle (Red Hat package): до 2.11.1-2.el8ap
python3.12-pycares (Red Hat package): до 4.4.0-3.el8ap
python3.12-pyasn1-modules (Red Hat package): до 0.3.0-2.el8ap
python3.12-pyasn1 (Red Hat package): до 0.5.1-2.el8ap
python3.12-pyOpenSSL (Red Hat package): до 24.1.0-2.el8ap
python3.12-pulpcore (Red Hat package): до 3.49.50-1.el8ap
python3.12-pulp-glue (Red Hat package): до 0.23.2-2.el8ap
python3.12-pulp-container (Red Hat package): до 2.19.3-2.el8ap
python3.12-pulp-ansible (Red Hat package): до 0.25.1-2.el8ap
python3.12-ptyprocess (Red Hat package): до 0.7.0-2.el8ap
python3.12-psycopg (Red Hat package): до 3.2.7-2.el8ap
python3.12-protobuf (Red Hat package): до 5.29.6-1.el8ap
python3.12-propcache (Red Hat package): до 0.4.1-1.el8ap
python3.12-prometheus-client (Red Hat package): до 0.19.0-2.el8ap
python3.12-podman (Red Hat package): до 5.4.0.1-2.el8ap
python3.12-pluggy (Red Hat package): до 1.6.0-2.el8ap
python3.12-platformdirs (Red Hat package): до 4.2.0-2.el8ap
python3.12-pillow (Red Hat package): до 10.3.0-2.el8ap
python3.12-pexpect (Red Hat package): до 4.9.0-2.el8ap
python3.12-persisting-theory (Red Hat package): до 1.0-3.el8ap
python3.12-pbr (Red Hat package): до 6.0.0-3.el8ap
python3.12-pathspec (Red Hat package): до 0.12.1-2.el8ap

python3.12-pathable (Red Hat package): до 0.4.3-2.el8ap
python3.12-parsley (Red Hat package): до 1.3-4.el8ap
python3.12-parse (Red Hat package): до 1.20.1-2.el8ap
python3.12-packaging (Red Hat package): до 23.2-2.el8
python3.12-opentelemetry-contrib (Red Hat package): до 1.28.0-1.el8ap
python3.12-opentelemetry (Red Hat package): до 1.28.0-1.el8ap
python3.12-openpyxl (Red Hat package): до 3.1.2-2.el8ap
python3.12-openapi-spec-validator (Red Hat package): до 0.7.1-2.el8ap
python3.12-openapi-schema-validator (Red Hat package): до 0.6.2-2.el8ap
python3.12-openapi-core (Red Hat package): до 0.19.1-2.el8ap
python3.12-onigurumacffi (Red Hat package): до 1.3.0-2.el8ap
python3.12-odfpy (Red Hat package): до 1.4.1-9.el8ap
python3.12-oauthlib (Red Hat package): до 3.2.2-2.el8ap
python3.12-nh3 (Red Hat package): до 0.2.18-2.el8ap
python3.12-netaddr (Red Hat package): до 1.2.1-2.el8ap
python3.12-mypy-extensions (Red Hat package): до 1.0.0-2.el8ap
python3.12-multidict (Red Hat package): до 6.0.4-2.el8ap
python3.12-more-itertools (Red Hat package): до 10.2.0-2.el8ap
python3.12-mccabe (Red Hat package): до 0.7.0-3.el8ap
python3.12-marshmallow (Red Hat package): до 3.26.2-1.el8ap
python3.12-markupsafe (Red Hat package): до 2.1.5-2.el8ap
python3.12-markuppy (Red Hat package): до 1.14-5.el8ap
python3.12-markdown (Red Hat package): до 3.5.2-2.el8ap
python3.12-lxml (Red Hat package): до 5.3.0-2.el8ap
python3.12-lockfile (Red Hat package): до 0.12.2-3.el8ap
python3.12-ldap-filter (Red Hat package): до 1.0.1-2.el8ap
python3.12-ldap (Red Hat package): до 3.4.5-1.el8ap
python3.12-lazy-object-proxy (Red Hat package): до 1.10.0-2.el8ap
python3.12-kubernetes (Red Hat package): до 26.1.0-3.el8ap
python3.12-jwcrypto (Red Hat package): до 1.5.6-2.el8ap
python3.12-jsonschema-specifications (Red Hat package): до 2023.12.1-2.el8ap
python3.12-jsonschema-path (Red Hat package): до 0.3.4-2.el8ap
python3.12-jsonschema (Red Hat package): до 4.21.1-2.el8ap
python3.12-json-stream-rs-tokenizer (Red Hat package): до 0.4.26-2.el8ap

python3.12-json-stream (Red Hat package): до 2.3.2-2.el8ap
python3.12-jq (Red Hat package): до 1.6.0-2.el8ap
python3.12-jpy (Red Hat package): до 0.15.0-2.el8ap
python3.12-jmespath (Red Hat package): до 1.0.1-3.el8ap
python3.12-jinja2 (Red Hat package): до 3.1.6-2.el8ap
python3.12-janus (Red Hat package): до 1.0.0-3.el8ap
python3.12-isodate (Red Hat package): до 0.6.1-3.el8ap
python3.12-insights-analytics-collector (Red Hat package): до 0.3.2-3.el8ap
python3.12-iniconfig (Red Hat package): до 2.0.0-2.el8ap
python3.12-inflection (Red Hat package): до 0.5.1-5.el8ap
python3.12-incremental (Red Hat package): до 24.7.2-2.el8ap
python3.12-importlib-metadata (Red Hat package): до 6.0.1-3.el8ap
python3.12-hyperlink (Red Hat package): до 21.0.0-3.el8ap
python3.12-gunicorn (Red Hat package): до 23.0.0-2.el8ap
python3.12-grpcio (Red Hat package): до 1.71.2-1.el8ap
python3.12-googleapis-common-protos (Red Hat package): до 1.72.0-1.el8ap
python3.12-google-auth (Red Hat package): до 2.27.0-2.el8ap
python3.12-gnupg (Red Hat package): до 0.5.2-2.el8ap
python3.12-gitpython (Red Hat package): до 3.1.41-2.el8ap
python3.12-gitdb (Red Hat package): до 4.0.11-2.el8ap
python3.12-galaxy-ng (Red Hat package): до 4.10.12-1.el8ap
python3.12-galaxy-importer (Red Hat package): до 0.4.37-3.el8ap
python3.12-frozenlist (Red Hat package): до 1.4.0-2.el8ap
python3.12-freezegun (Red Hat package): до 1.5.5-1.el8ap
python3.12-flake8 (Red Hat package): до 6.1.0-3.el8ap
python3.12-filelock (Red Hat package): до 3.13.1-2.el8ap
python3.12-execnet (Red Hat package): до 2.1.2-2.el8ap
python3.12-et-xmlfile (Red Hat package): до 1.1.0-4.el8ap
python3.12-enrich (Red Hat package): до 1.2.7-3.el8ap
python3.12-ecdsa (Red Hat package): до 0.18.0-2.el8ap
python3.12-dynaconf (Red Hat package): до 3.2.11-2.el8ap
python3.12-drools-jpy (Red Hat package): до 0.3.10-2.el8ap
python3.12-drf-spectacular (Red Hat package): до 0.26.5-3.el8ap
python3.12-drf-nested-routers (Red Hat package): до 0.93.5-2.el8ap

python3.12-drf-access-policy (Red Hat package): до 1.5.0-2.el8ap
python3.12-dpath (Red Hat package): до 2.1.6-2.el8ap
python3.12-djangorestframework-queryfields (Red Hat package): до 1.1.0-2.el8ap
python3.12-djangorestframework (Red Hat package): до 3.15.1-2.el8ap
python3.12-django-split-settings (Red Hat package): до 1.2.0-3.el8ap
python3.12-django-rq (Red Hat package): до 3.2.2-1.el8ap
python3.12-django-redis (Red Hat package): до 5.4.0-2.el8ap
python3.12-django-prometheus (Red Hat package): до 2.3.1-3.el8ap
python3.12-django-picklefield (Red Hat package): до 3.1-2.el8ap
python3.12-django-oauth-toolkit (Red Hat package): до 2.3.0-2.el8ap
python3.12-django-lifecycle (Red Hat package): до 1.1.2-2.el8ap
python3.12-django-ipware (Red Hat package): до 3.0.7-4.el8ap
python3.12-django-import-export (Red Hat package): до 3.3.6-3.el8ap
python3.12-django-guid (Red Hat package): до 3.4.0-2.el8ap
python3.12-django-flags (Red Hat package): до 5.0.13-2.el8ap
python3.12-django-filter (Red Hat package): до 23.5-2.el8ap
python3.12-django-extensions (Red Hat package): до 4.1-2.el8ap
python3.12-django-dynamic-preferences (Red Hat package): до 1.16.0-2.el8ap
python3.12-django-crum (Red Hat package): до 0.7.9-3.el8ap
python3.12-django-auth-ldap (Red Hat package): до 4.0.0-3.el8ap
python3.12-django-ansible-base (Red Hat package): до 2.5.20260225-1.el8ap
python3.12-django (Red Hat package): до 4.2.28-1.el8ap
python3.12-distro (Red Hat package): до 1.9.0-2.el8ap
python3.12-distlib (Red Hat package): до 0.4.0-2.el8ap
python3.12-dispatcherd (Red Hat package): до 2025.5.19-3.el8ap
python3.12-diff-match-patch (Red Hat package): до 20230430-2.el8ap
python3.12-deprecated (Red Hat package): до 1.2.14-2.el8ap
python3.12-defusedxml (Red Hat package): до 0.7.1-5.el8ap
python3.12-dateutil (Red Hat package): до 2.8.2-3.el8ap
python3.12-daphne (Red Hat package): до 4.0.0-4.el8ap
python3.12-daemon (Red Hat package): до 3.1.2-3.el8ap
python3.12-cryptography (Red Hat package): до 42.0.5-2.el8ap
python3.12-crontab (Red Hat package): до 1.0.5-1.el8ap
python3.12-croniter (Red Hat package): до 2.0.1-2.el8ap

python3.12-constantly (Red Hat package): до 23.10.4-1.el8ap
python3.12-commonmark (Red Hat package): до 0.9.1-7.el8ap
python3.12-colorama (Red Hat package): до 0.4.6-2.el8ap
python3.12-click-help-colors (Red Hat package): до 0.9.4-2.el8ap
python3.12-click (Red Hat package): до 8.1.7-2.el8ap
python3.12-chardet (Red Hat package): до 5.2.0-3.el8ap
python3.12-channels (Red Hat package): до 4.0.0-4.el8ap
python3.12-certifi (Red Hat package): до 2023.5.7-2.el8ap
python3.12-cachetools (Red Hat package): до 5.3.2-2.el8ap
python3.12-brotli (Red Hat package): до 1.2.0-1.el8ap
python3.12-bracex (Red Hat package): до 2.4-2.el8ap
python3.12-botocore (Red Hat package): до 1.34.162-2.el8ap
python3.12-boto3 (Red Hat package): до 1.34.30-2.el8ap
python3.12-black (Red Hat package): до 24.4.2-3.el8ap
python3.12-backoff (Red Hat package): до 2.2.1-2.el8ap
python3.12-azure-core (Red Hat package): до 1.34.0-2.el8ap
python3.12-autobahn (Red Hat package): до 24.4.2-2.el8ap
python3.12-attrs (Red Hat package): до 22.2.0-2.el8ap
python3.12-asyncio-throttle (Red Hat package): до 1.0.2-5.el8ap
python3.12-async-lru (Red Hat package): до 2.0.5-1.el8ap
python3.12-asgiref (Red Hat package): до 3.7.2-2.el8ap
python3.12-argon2-cffi-bindings (Red Hat package): до 21.2.0-2.el8ap
python3.12-argon2-cffi (Red Hat package): до 23.1.0-2.el8ap
python3.12-ansible-sdk (Red Hat package): до 1.0.0-3.el8ap
python3.12-ansible-pylibssh (Red Hat package): до 1.2.2-2.el8ap
python3.12-ansible-compat (Red Hat package): до 25.12.0-3.el8ap
python3.12-aiosignal (Red Hat package): до 1.4.0-1.el8ap
python3.12-aiohttp (Red Hat package): до 3.13.3-2.el8ap
python3.12-aiohappyeyeballs (Red Hat package): до 2.6.1-1.el8ap
python3.12-aiofiles (Red Hat package): до 23.2.1-2.el8ap
python3.12-aiodns (Red Hat package): до 3.2.0-2.el8ap
python3.12-Automat (Red Hat package): до 22.10.0-4.el8ap
pulpcore-selinux (Red Hat package): до 2.0.1-2.el8ap
molecule (Red Hat package): до 25.12.0-2.el8ap

bindep (Red Hat package): до 2.13.0-2.el8ap
automation-hub (Red Hat package): до 4.10.12-1.el8ap
automation-gateway (Red Hat package): до 2.5.20260225-1.el8ap
automation-eda-controller (Red Hat package): до 1.1.16-1.el8ap
automation-controller-fapolicyd (Red Hat package): до 1.0-6.el8ap
automation-controller (Red Hat package): до 4.6.26-1.el8ap
ansible-sign (Red Hat package): до 0.1.4-2.el8ap
ansible-runner (Red Hat package): до 2.4.2-3.el8ap
ansible-rulebook (Red Hat package): до 1.1.7-2.el8ap
ansible-navigator (Red Hat package): до 26.1.1-1.1.el8ap
ansible-lint (Red Hat package): до 26.1.0-3.el8ap
ansible-dev-tools (Red Hat package): до 26.1.0-3.el8ap
ansible-dev-environment (Red Hat package): до 25.12.2-1.2.el8ap
ansible-creator (Red Hat package): до 25.12.0-1.1.el8ap
ansible-core (Red Hat package): до 2.16.16-1.el8ap
ansible-builder (Red Hat package): до 3.1.1-1.2.el8ap
ansible-automation-platform-installer (Red Hat package): до 2.5-21.el8ap
aap-metrics-utility (Red Hat package): до 0.6.0-2.1.el8ap
python3.12-wheel (Red Hat package): до 0.41.2-4.el8_10
python3.12-setuptools (Red Hat package): до 68.2.2-5.el9_6
Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: Межсайтовый скриптинг

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

Оценка CVSSv3: 8.0 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2026:3959

95

Краткое описание: Отказ в обслуживании в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2026-23490

Идентификатор программной ошибки: CWE-770 Выделение ресурсов без ограничений или регулировки

Уязвимый продукт: python3.12-django-storages (Red Hat package): до 1.14.2-3.el8ap
python3.12-azure-storage-blob (Red Hat package): до 12.19.0-2.el8ap
yamllint (Red Hat package): до 1.35.1-2.el8ap
uwsgi (Red Hat package): до 2.0.28-2.el8ap
supervisor (Red Hat package): до 4.2.5-2.el8ap
receptor (Red Hat package): до 1.6.3-4.el8ap
python3.12-zope-interface (Red Hat package): до 6.1-2.el8ap
python3.12-zipp (Red Hat package): до 3.19.2-2.el8ap
python3.12-yarl (Red Hat package): до 1.18.3-1.el8ap
python3.12-xxhash (Red Hat package): до 3.4.1-2.el8ap
python3.12-xmlsec (Red Hat package): до 1.3.13-3.el8ap
python3.12-xlwt (Red Hat package): до 1.3.0-5.el8ap
python3.12-xlrd (Red Hat package): до 2.0.1-7.el8ap
python3.12-xds-protos (Red Hat package): до 1.71.2-1.el8ap
python3.12-wrapt (Red Hat package): до 1.16.0-2.el8ap
python3.12-whitenoise (Red Hat package): до 6.6.0-2.el8ap
python3.12-werkzeug (Red Hat package): до 3.0.3-2.el8ap
python3.12-websockets (Red Hat package): до 15.0-3.el8ap
python3.12-websocket-client (Red Hat package): до 1.7.0-3.el8ap
python3.12-wcmatch (Red Hat package): до 8.5-2.el8ap
python3.12-watchdog (Red Hat package): до 5.0.2-2.el8ap
python3.12-virtualenv (Red Hat package): до 20.25.1-2.el8ap
python3.12-validators (Red Hat package): до 0.34.0-2.el8ap
python3.12-uuid6 (Red Hat package): до 2024.1.12-2.el8ap
python3.12-urllib3 (Red Hat package): до 2.6.3-2.el8ap
python3.12-url-normalize (Red Hat package): до 1.4.3-6.el8ap
python3.12-uritemplate (Red Hat package): до 4.1.1-4.el8ap
python3.12-uamqp (Red Hat package): до 1.6.8-2.el8ap
python3.12-typing-extensions (Red Hat package): до 4.15.0-2.el8ap
python3.12-txaio (Red Hat package): до 23.1.1-3.el8ap

python3.12-twisted (Red Hat package): до 24.7.0-2.el8ap
python3.12-tox-ansible (Red Hat package): до 25.12.0-2.el8ap
python3.12-tox (Red Hat package): до 4.15.1-2.el8ap
python3.12-termcolor (Red Hat package): до 3.1.0-2.el8ap
python3.12-tacacs-plus (Red Hat package): до 2.6-3.el8ap
python3.12-tabulate (Red Hat package): до 0.9.0-4.el8ap
python3.12-tablib (Red Hat package): до 3.5.0-2.el8ap
python3.12-subprocess-tee (Red Hat package): до 0.4.2-2.el8ap
python3.12-sqlparse (Red Hat package): до 0.5.3-3.el8ap
python3.12-social-auth-core (Red Hat package): до 4.5.4-2.el8ap
python3.12-social-auth-app-django (Red Hat package): до 5.4.1-2.el8ap
python3.12-smmap (Red Hat package): до 5.0.1-2.el8ap
python3.12-six (Red Hat package): до 1.17.0-1.el8ap
python3.12-service-identity (Red Hat package): до 21.1.0-3.el8ap
python3.12-semantic-version (Red Hat package): до 2.10.0-3.el8ap
python3.12-s3transfer (Red Hat package): до 0.10.0-2.el8ap
python3.12-ruamel-yaml-clib (Red Hat package): до 0.2.15-2.el8ap
python3.12-ruamel-yaml (Red Hat package): до 0.18.15-2.el8ap
python3.12-rsa (Red Hat package): до 4.9-3.el8ap
python3.12-rq-scheduler (Red Hat package): до 0.14.0-1.el8ap
python3.12-rq (Red Hat package): до 2.6.1-1.el8ap
python3.12-rpds-py (Red Hat package): до 0.18.1-3.el8ap
python3.12-rich (Red Hat package): до 13.1.0-2.el8ap
python3.12-rfc3339-validator (Red Hat package): до 0.1.4-2.el8ap
python3.12-resolvelib (Red Hat package): до 1.0.1-2.el8ap
python3.12-requests-oauthlib (Red Hat package): до 1.3.1-2.el8ap
python3.12-requests (Red Hat package): до 2.31.0-4.el8ap
python3.12-referencing (Red Hat package): до 0.36.2-3.el8ap
python3.12-redis (Red Hat package): до 4.6.0-3.el8ap
python3.12-pytz (Red Hat package): до 2024.1-2.el8ap
python3.12-python3-saml (Red Hat package): до 1.16.0-3.el8ap
python3.12-python3-openid (Red Hat package): до 3.2.0-4.el8ap
python3.12-pytest-xdist (Red Hat package): до 3.8.0-2.el8ap
python3.12-pytest-sugar (Red Hat package): до 1.1.1-2.el8ap

python3.12-pytest-plus (Red Hat package): до 0.8.1-2.el8ap
python3.12-pytest-ansible (Red Hat package): до 25.12.0-2.el8ap
python3.12-pytest (Red Hat package): до 9.0.1-2.el8ap
python3.12-pyrad (Red Hat package): до 2.4-3.el8ap
python3.12-pyproject-api (Red Hat package): до 1.6.1-2.el8ap
python3.12-pyparsing (Red Hat package): до 3.1.1-2.el8ap
python3.12-pyjwt (Red Hat package): до 2.7.0-3.el8ap
python3.12-pygtrie (Red Hat package): до 2.5.0-3.el8ap
python3.12-pygments (Red Hat package): до 2.17.2-3.el8ap
python3.12-pyflakes (Red Hat package): до 3.1.0-2.el8ap
python3.12-pydantic (Red Hat package): до 1.10.15-2.el8ap
python3.12-pycodestyle (Red Hat package): до 2.11.1-2.el8ap
python3.12-pycares (Red Hat package): до 4.4.0-3.el8ap
python3.12-pyasn1-modules (Red Hat package): до 0.3.0-2.el8ap
python3.12-pyasn1 (Red Hat package): до 0.5.1-2.el8ap
python3.12-pyOpenSSL (Red Hat package): до 24.1.0-2.el8ap
python3.12-pulpcore (Red Hat package): до 3.49.50-1.el8ap
python3.12-pulp-glue (Red Hat package): до 0.23.2-2.el8ap
python3.12-pulp-container (Red Hat package): до 2.19.3-2.el8ap
python3.12-pulp-ansible (Red Hat package): до 0.25.1-2.el8ap
python3.12-ptyprocess (Red Hat package): до 0.7.0-2.el8ap
python3.12-psycopg (Red Hat package): до 3.2.7-2.el8ap
python3.12-protobuf (Red Hat package): до 5.29.6-1.el8ap
python3.12-propcache (Red Hat package): до 0.4.1-1.el8ap
python3.12-prometheus-client (Red Hat package): до 0.19.0-2.el8ap
python3.12-podman (Red Hat package): до 5.4.0.1-2.el8ap
python3.12-pluggy (Red Hat package): до 1.6.0-2.el8ap
python3.12-platformdirs (Red Hat package): до 4.2.0-2.el8ap
python3.12-pillow (Red Hat package): до 10.3.0-2.el8ap
python3.12-pexpect (Red Hat package): до 4.9.0-2.el8ap
python3.12-persisting-theory (Red Hat package): до 1.0-3.el8ap
python3.12-pbr (Red Hat package): до 6.0.0-3.el8ap
python3.12-pathspec (Red Hat package): до 0.12.1-2.el8ap
python3.12-pathable (Red Hat package): до 0.4.3-2.el8ap

python3.12-parsley (Red Hat package): до 1.3-4.el8ap
python3.12-parse (Red Hat package): до 1.20.1-2.el8ap
python3.12-packaging (Red Hat package): до 23.2-2.el8
python3.12-opentelemetry-contrib (Red Hat package): до 1.28.0-1.el8ap
python3.12-opentelemetry (Red Hat package): до 1.28.0-1.el8ap
python3.12-openpyxl (Red Hat package): до 3.1.2-2.el8ap
python3.12-openapi-spec-validator (Red Hat package): до 0.7.1-2.el8ap
python3.12-openapi-schema-validator (Red Hat package): до 0.6.2-2.el8ap
python3.12-openapi-core (Red Hat package): до 0.19.1-2.el8ap
python3.12-onigurumacffi (Red Hat package): до 1.3.0-2.el8ap
python3.12-odfpy (Red Hat package): до 1.4.1-9.el8ap
python3.12-oauthlib (Red Hat package): до 3.2.2-2.el8ap
python3.12-nh3 (Red Hat package): до 0.2.18-2.el8ap
python3.12-netaddr (Red Hat package): до 1.2.1-2.el8ap
python3.12-mypy-extensions (Red Hat package): до 1.0.0-2.el8ap
python3.12-multidict (Red Hat package): до 6.0.4-2.el8ap
python3.12-more-itertools (Red Hat package): до 10.2.0-2.el8ap
python3.12-mccabe (Red Hat package): до 0.7.0-3.el8ap
python3.12-marshmallow (Red Hat package): до 3.26.2-1.el8ap
python3.12-markupsafe (Red Hat package): до 2.1.5-2.el8ap
python3.12-markuppy (Red Hat package): до 1.14-5.el8ap
python3.12-markdown (Red Hat package): до 3.5.2-2.el8ap
python3.12-lxml (Red Hat package): до 5.3.0-2.el8ap
python3.12-lockfile (Red Hat package): до 0.12.2-3.el8ap
python3.12-ldap-filter (Red Hat package): до 1.0.1-2.el8ap
python3.12-ldap (Red Hat package): до 3.4.5-1.el8ap
python3.12-lazy-object-proxy (Red Hat package): до 1.10.0-2.el8ap
python3.12-kubernetes (Red Hat package): до 26.1.0-3.el8ap
python3.12-jwcrypto (Red Hat package): до 1.5.6-2.el8ap
python3.12-jsonschema-specifications (Red Hat package): до 2023.12.1-2.el8ap
python3.12-jsonschema-path (Red Hat package): до 0.3.4-2.el8ap
python3.12-jsonschema (Red Hat package): до 4.21.1-2.el8ap
python3.12-json-stream-rs-tokenizer (Red Hat package): до 0.4.26-2.el8ap
python3.12-json-stream (Red Hat package): до 2.3.2-2.el8ap

python3.12-jq (Red Hat package): до 1.6.0-2.el8ap
python3.12-jpy (Red Hat package): до 0.15.0-2.el8ap
python3.12-jmespath (Red Hat package): до 1.0.1-3.el8ap
python3.12-jinja2 (Red Hat package): до 3.1.6-2.el8ap
python3.12-janus (Red Hat package): до 1.0.0-3.el8ap
python3.12-isodate (Red Hat package): до 0.6.1-3.el8ap
python3.12-insights-analytics-collector (Red Hat package): до 0.3.2-3.el8ap
python3.12-iniconfig (Red Hat package): до 2.0.0-2.el8ap
python3.12-inflection (Red Hat package): до 0.5.1-5.el8ap
python3.12-incremental (Red Hat package): до 24.7.2-2.el8ap
python3.12-importlib-metadata (Red Hat package): до 6.0.1-3.el8ap
python3.12-hyperlink (Red Hat package): до 21.0.0-3.el8ap
python3.12-gunicorn (Red Hat package): до 23.0.0-2.el8ap
python3.12-grpcio (Red Hat package): до 1.71.2-1.el8ap
python3.12-googleapis-common-protos (Red Hat package): до 1.72.0-1.el8ap
python3.12-google-auth (Red Hat package): до 2.27.0-2.el8ap
python3.12-gnupg (Red Hat package): до 0.5.2-2.el8ap
python3.12-gitpython (Red Hat package): до 3.1.41-2.el8ap
python3.12-gitdb (Red Hat package): до 4.0.11-2.el8ap
python3.12-galaxy-ng (Red Hat package): до 4.10.12-1.el8ap
python3.12-galaxy-importer (Red Hat package): до 0.4.37-3.el8ap
python3.12-frozenlist (Red Hat package): до 1.4.0-2.el8ap
python3.12-freezegun (Red Hat package): до 1.5.5-1.el8ap
python3.12-flake8 (Red Hat package): до 6.1.0-3.el8ap
python3.12-filelock (Red Hat package): до 3.13.1-2.el8ap
python3.12-execnet (Red Hat package): до 2.1.2-2.el8ap
python3.12-et-xmlfile (Red Hat package): до 1.1.0-4.el8ap
python3.12-enrich (Red Hat package): до 1.2.7-3.el8ap
python3.12-ecdsa (Red Hat package): до 0.18.0-2.el8ap
python3.12-dynaconf (Red Hat package): до 3.2.11-2.el8ap
python3.12-drools-jpy (Red Hat package): до 0.3.10-2.el8ap
python3.12-drf-spectacular (Red Hat package): до 0.26.5-3.el8ap
python3.12-drf-nested-routers (Red Hat package): до 0.93.5-2.el8ap
python3.12-drf-access-policy (Red Hat package): до 1.5.0-2.el8ap

python3.12-dpath (Red Hat package): до 2.1.6-2.el8ap
python3.12-djangorestframework-queryfields (Red Hat package): до 1.1.0-2.el8ap
python3.12-djangorestframework (Red Hat package): до 3.15.1-2.el8ap
python3.12-django-split-settings (Red Hat package): до 1.2.0-3.el8ap
python3.12-django-rq (Red Hat package): до 3.2.2-1.el8ap
python3.12-django-redis (Red Hat package): до 5.4.0-2.el8ap
python3.12-django-prometheus (Red Hat package): до 2.3.1-3.el8ap
python3.12-django-picklefield (Red Hat package): до 3.1-2.el8ap
python3.12-django-oauth-toolkit (Red Hat package): до 2.3.0-2.el8ap
python3.12-django-lifecycle (Red Hat package): до 1.1.2-2.el8ap
python3.12-django-ipware (Red Hat package): до 3.0.7-4.el8ap
python3.12-django-import-export (Red Hat package): до 3.3.6-3.el8ap
python3.12-django-guid (Red Hat package): до 3.4.0-2.el8ap
python3.12-django-flags (Red Hat package): до 5.0.13-2.el8ap
python3.12-django-filter (Red Hat package): до 23.5-2.el8ap
python3.12-django-extensions (Red Hat package): до 4.1-2.el8ap
python3.12-django-dynamic-preferences (Red Hat package): до 1.16.0-2.el8ap
python3.12-django-crum (Red Hat package): до 0.7.9-3.el8ap
python3.12-django-auth-ldap (Red Hat package): до 4.0.0-3.el8ap
python3.12-django-ansible-base (Red Hat package): до 2.5.20260225-1.el8ap
python3.12-django (Red Hat package): до 4.2.28-1.el8ap
python3.12-distro (Red Hat package): до 1.9.0-2.el8ap
python3.12-distlib (Red Hat package): до 0.4.0-2.el8ap
python3.12-dispatcherd (Red Hat package): до 2025.5.19-3.el8ap
python3.12-diff-match-patch (Red Hat package): до 20230430-2.el8ap
python3.12-deprecated (Red Hat package): до 1.2.14-2.el8ap
python3.12-defusedxml (Red Hat package): до 0.7.1-5.el8ap
python3.12-dateutil (Red Hat package): до 2.8.2-3.el8ap
python3.12-daphne (Red Hat package): до 4.0.0-4.el8ap
python3.12-daemon (Red Hat package): до 3.1.2-3.el8ap
python3.12-cryptography (Red Hat package): до 42.0.5-2.el8ap
python3.12-crontab (Red Hat package): до 1.0.5-1.el8ap
python3.12-croniter (Red Hat package): до 2.0.1-2.el8ap
python3.12-constantly (Red Hat package): до 23.10.4-1.el8ap

python3.12-commonmark (Red Hat package): до 0.9.1-7.el8ap
python3.12-colorama (Red Hat package): до 0.4.6-2.el8ap
python3.12-click-help-colors (Red Hat package): до 0.9.4-2.el8ap
python3.12-click (Red Hat package): до 8.1.7-2.el8ap
python3.12-chardet (Red Hat package): до 5.2.0-3.el8ap
python3.12-channels (Red Hat package): до 4.0.0-4.el8ap
python3.12-certifi (Red Hat package): до 2023.5.7-2.el8ap
python3.12-cachetools (Red Hat package): до 5.3.2-2.el8ap
python3.12-brotli (Red Hat package): до 1.2.0-1.el8ap
python3.12-bracex (Red Hat package): до 2.4-2.el8ap
python3.12-botocore (Red Hat package): до 1.34.162-2.el8ap
python3.12-boto3 (Red Hat package): до 1.34.30-2.el8ap
python3.12-black (Red Hat package): до 24.4.2-3.el8ap
python3.12-backoff (Red Hat package): до 2.2.1-2.el8ap
python3.12-azure-core (Red Hat package): до 1.34.0-2.el8ap
python3.12-autobahn (Red Hat package): до 24.4.2-2.el8ap
python3.12-attrs (Red Hat package): до 22.2.0-2.el8ap
python3.12-asyncio-throttle (Red Hat package): до 1.0.2-5.el8ap
python3.12-async-lru (Red Hat package): до 2.0.5-1.el8ap
python3.12-asgiref (Red Hat package): до 3.7.2-2.el8ap
python3.12-argon2-cffi-bindings (Red Hat package): до 21.2.0-2.el8ap
python3.12-argon2-cffi (Red Hat package): до 23.1.0-2.el8ap
python3.12-ansible-sdk (Red Hat package): до 1.0.0-3.el8ap
python3.12-ansible-pylibssh (Red Hat package): до 1.2.2-2.el8ap
python3.12-ansible-compat (Red Hat package): до 25.12.0-3.el8ap
python3.12-aiosignal (Red Hat package): до 1.4.0-1.el8ap
python3.12-aiohttp (Red Hat package): до 3.13.3-2.el8ap
python3.12-aiohappyeyeballs (Red Hat package): до 2.6.1-1.el8ap
python3.12-aiofiles (Red Hat package): до 23.2.1-2.el8ap
python3.12-aiodns (Red Hat package): до 3.2.0-2.el8ap
python3.12-Automat (Red Hat package): до 22.10.0-4.el8ap
pulpcore-selinux (Red Hat package): до 2.0.1-2.el8ap
molecule (Red Hat package): до 25.12.0-2.el8ap
bindep (Red Hat package): до 2.13.0-2.el8ap

automation-hub (Red Hat package): до 4.10.12-1.el8ap
automation-gateway (Red Hat package): до 2.5.20260225-1.el8ap
automation-eda-controller (Red Hat package): до 1.1.16-1.el8ap
automation-controller-fapolicyd (Red Hat package): до 1.0-6.el8ap
automation-controller (Red Hat package): до 4.6.26-1.el8ap
ansible-sign (Red Hat package): до 0.1.4-2.el8ap
ansible-runner (Red Hat package): до 2.4.2-3.el8ap
ansible-rulebook (Red Hat package): до 1.1.7-2.el8ap
ansible-navigator (Red Hat package): до 26.1.1-1.1.el8ap
ansible-lint (Red Hat package): до 26.1.0-3.el8ap
ansible-dev-tools (Red Hat package): до 26.1.0-3.el8ap
ansible-dev-environment (Red Hat package): до 25.12.2-1.2.el8ap
ansible-creator (Red Hat package): до 25.12.0-1.1.el8ap
ansible-core (Red Hat package): до 2.16.16-1.el8ap
ansible-builder (Red Hat package): до 3.1.1-1.2.el8ap
ansible-automation-platform-installer (Red Hat package): до 2.5-21.el8ap
aap-metrics-utility (Red Hat package): до 0.6.0-2.1.el8ap
python3.12-wheel (Red Hat package): до 0.41.2-4.el8_10
python3.12-setuptools (Red Hat package): до 68.2.2-5.el9_6
Ansible Automation Platform: до 2.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

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: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2026:3959

96

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

Идентификатор уязвимости: CVE-2026-3779

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Foxit PDF Reader for Mac: 2023.1.0.55583 - 2025.3.0.69570
Foxit PDF Editor for Mac (formerly PhantomPDF): 13.0.0.61829 - 2025.3.0.69570

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Editor+for+Mac+2026.1%2F14.0.3%2F13.2.3+and+Foxit+PDF+Reader+for+Mac+2026.12026-03-31+00%3A00%3A00

97

Краткое описание: Получение конфиденциальной информации в FUJI Electric V-SFT

Идентификатор уязвимости: CVE-2026-32929

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Monitouch V-SFT: 6.2.2.0 - 6.2.10

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 8.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://jvn.jp/en/vu/JVNVU90448293/index.html

98

Краткое описание: Выполнение произвольного кода в FUJI Electric V-SFT

Идентификатор уязвимости: CVE-2026-32928

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Monitouch V-SFT: 6.2.2.0 - 6.2.10

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Переполнение буфера.

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: 8.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://jvn.jp/en/vu/JVNVU90448293/index.html

99

Краткое описание: Получение конфиденциальной информации в FUJI Electric V-SFT

Идентификатор уязвимости: CVE-2026-32927

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Monitouch V-SFT: 6.2.2.0 - 6.2.10

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 8.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://jvn.jp/en/vu/JVNVU90448293/index.html

100

Краткое описание: Получение конфиденциальной информации в FUJI Electric V-SFT

Идентификатор уязвимости: CVE-2026-32926

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Monitouch V-SFT: 6.2.2.0 - 6.2.10

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 8.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://jvn.jp/en/vu/JVNVU90448293/index.html

101

Краткое описание: Выполнение произвольного кода в FUJI Electric V-SFT

Идентификатор уязвимости: CVE-2026-32925

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Monitouch V-SFT: 6.2.2.0 - 6.2.10

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Переполнение буфера.

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: 8.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://jvn.jp/en/vu/JVNVU90448293/index.html

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-5272

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.167

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

10
2

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
- https://crbug.com/492228019
- https://crbug.com/492213293
- https://crbug.com/490118036
- https://crbug.com/496205576
- https://crbug.com/495931147
- https://crbug.com/495507390
- https://crbug.com/494644471
- https://crbug.com/493900619
- https://crbug.com/492139412
- https://crbug.com/493952652
- https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

103

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-5274

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.167

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: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
- https://crbug.com/492228019
- https://crbug.com/492213293
- https://crbug.com/490118036
- https://crbug.com/496205576
- https://crbug.com/495931147
- https://crbug.com/495507390
- https://crbug.com/494644471
- https://crbug.com/493900619
- https://crbug.com/492139412
- https://crbug.com/493952652
- https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

104	**Краткое описание:** Выполнение произвольного кода в Google Chrome **Идентификатор уязвимости:** CVE-2026-5275 **Идентификатор программной ошибки:** CWE-122 Переполнение буфера в динамической памяти **Уязвимый продукт:** Google Chrome: 100.0.4896.60 - 146.0.7680.167 **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:** 2026-04-01 / 2026-04-01 **Ссылки на источник:** • https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html • https://crbug.com/492228019 • https://crbug.com/492213293 • https://crbug.com/490118036 • https://crbug.com/496205576 • https://crbug.com/495931147 • https://crbug.com/495507390 • https://crbug.com/494644471 • https://crbug.com/493900619 • https://crbug.com/492139412 • https://crbug.com/493952652 • https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

105

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-5277

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.167

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: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
- https://crbug.com/492228019
- https://crbug.com/492213293
- https://crbug.com/490118036
- https://crbug.com/496205576
- https://crbug.com/495931147
- https://crbug.com/495507390
- https://crbug.com/494644471
- https://crbug.com/493900619
- https://crbug.com/492139412
- https://crbug.com/493952652
- https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

106	**Краткое описание:** Выполнение произвольного кода в Google Chrome **Идентификатор уязвимости:** CVE-2026-5278 **Идентификатор программной ошибки:** CWE-416 Использование после освобождения **Уязвимый продукт:** Google Chrome: 100.0.4896.60 - 146.0.7680.167 **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:** 2026-04-01 / 2026-04-01 **Ссылки на источник:** • https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html • https://crbug.com/492228019 • https://crbug.com/492213293 • https://crbug.com/490118036 • https://crbug.com/496205576 • https://crbug.com/495931147 • https://crbug.com/495507390 • https://crbug.com/494644471 • https://crbug.com/493900619 • https://crbug.com/492139412 • https://crbug.com/493952652 • https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-5279

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.167

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

10 7 **Оценка CVSSv4:** Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
- https://crbug.com/492228019
- https://crbug.com/492213293
- https://crbug.com/490118036
- https://crbug.com/496205576
- https://crbug.com/495931147
- https://crbug.com/495507390
- https://crbug.com/494644471
- https://crbug.com/493900619
- https://crbug.com/492139412
- https://crbug.com/493952652

- https://crbug.com/492131521
- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

108

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-5280

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.167

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: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
- https://crbug.com/492228019
- https://crbug.com/492213293
- https://crbug.com/490118036
- https://crbug.com/496205576
- https://crbug.com/495931147
- https://crbug.com/495507390
- https://crbug.com/494644471
- https://crbug.com/493900619
- https://crbug.com/492139412
- https://crbug.com/493952652
- https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

109

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-5281

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.167

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: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
- https://crbug.com/492228019
- https://crbug.com/492213293
- https://crbug.com/490118036
- https://crbug.com/496205576
- https://crbug.com/495931147
- https://crbug.com/495507390
- https://crbug.com/494644471
- https://crbug.com/493900619
- https://crbug.com/492139412
- https://crbug.com/493952652
- https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

110	**Краткое описание:** Получение конфиденциальной информации в Google Chrome **Идентификатор уязвимости:** CVE-2026-5282 **Идентификатор программной ошибки:** CWE-125 Чтение за пределами буфера **Уязвимый продукт:** Google Chrome: 100.0.4896.60 - 146.0.7680.167 **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:N/A:H **Оценка CVSSv4:** Не определено **Вектор атаки:** Сетевой **Взаимодействие с пользователем:** Требуется **Дата выявления / Дата обновления:** 2026-04-01 / 2026-04-01 **Ссылки на источник:** • https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html • https://crbug.com/492228019 • https://crbug.com/492213293 • https://crbug.com/490118036 • https://crbug.com/496205576 • https://crbug.com/495931147 • https://crbug.com/495507390 • https://crbug.com/494644471 • https://crbug.com/493900619 • https://crbug.com/492139412 • https://crbug.com/493952652 • https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

111

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-5284

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.167

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: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
- https://crbug.com/492228019
- https://crbug.com/492213293
- https://crbug.com/490118036
- https://crbug.com/496205576
- https://crbug.com/495931147
- https://crbug.com/495507390
- https://crbug.com/494644471
- https://crbug.com/493900619
- https://crbug.com/492139412
- https://crbug.com/493952652
- https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-5286

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.167

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

11
2

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
- https://crbug.com/492228019
- https://crbug.com/492213293
- https://crbug.com/490118036
- https://crbug.com/496205576
- https://crbug.com/495931147
- https://crbug.com/495507390
- https://crbug.com/494644471
- https://crbug.com/493900619
- https://crbug.com/492139412
- https://crbug.com/493952652
- https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-5287

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.167

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

11
3

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
- https://crbug.com/492228019
- https://crbug.com/492213293
- https://crbug.com/490118036
- https://crbug.com/496205576
- https://crbug.com/495931147
- https://crbug.com/495507390
- https://crbug.com/494644471
- https://crbug.com/493900619
- https://crbug.com/492139412
- https://crbug.com/493952652
- https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

114

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-5288

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.167

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: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
- https://crbug.com/492228019
- https://crbug.com/492213293
- https://crbug.com/490118036
- https://crbug.com/496205576
- https://crbug.com/495931147
- https://crbug.com/495507390
- https://crbug.com/494644471
- https://crbug.com/493900619
- https://crbug.com/492139412
- https://crbug.com/493952652
- https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-5289

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.167

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

115

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-01 / 2026-04-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html
- https://crbug.com/492228019
- https://crbug.com/492213293
- https://crbug.com/490118036
- https://crbug.com/496205576
- https://crbug.com/495931147
- https://crbug.com/495507390
- https://crbug.com/494644471
- https://crbug.com/493900619
- https://crbug.com/492139412
- https://crbug.com/493952652
- https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

116	**Краткое описание:** Выполнение произвольного кода в Google Chrome **Идентификатор уязвимости:** CVE-2026-5290 **Идентификатор программной ошибки:** CWE-416 Использование после освобождения **Уязвимый продукт:** Google Chrome: 100.0.4896.60 - 146.0.7680.167 **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:** 2026-04-01 / 2026-04-01 **Ссылки на источник:** • https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html • https://crbug.com/492228019 • https://crbug.com/492213293 • https://crbug.com/490118036 • https://crbug.com/496205576 • https://crbug.com/495931147 • https://crbug.com/495507390 • https://crbug.com/494644471 • https://crbug.com/493900619 • https://crbug.com/492139412 • https://crbug.com/493952652 • https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

117	**Краткое описание:** Получение конфиденциальной информации в Google Chrome **Идентификатор уязвимости:** CVE-2026-5292 **Идентификатор программной ошибки:** CWE-125 Чтение за пределами буфера **Уязвимый продукт:** Google Chrome: 100.0.4896.60 - 146.0.7680.167 **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:** 2026-04-01 / 2026-04-01 **Ссылки на источник:** • https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html • https://crbug.com/492228019 • https://crbug.com/492213293 • https://crbug.com/490118036 • https://crbug.com/496205576 • https://crbug.com/495931147 • https://crbug.com/495507390 • https://crbug.com/494644471 • https://crbug.com/493900619 • https://crbug.com/492139412 • https://crbug.com/493952652 • https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188

118	**Краткое описание:** Выполнение произвольного кода в Google Chrome **Идентификатор уязвимости:** CVE-2026-5285 **Идентификатор программной ошибки:** CWE-416 Использование после освобождения **Уязвимый продукт:** Google Chrome: 100.0.4896.60 - 146.0.7680.167 **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:** 2026-04-01 / 2026-04-01 **Ссылки на источник:** • https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_31.html • https://crbug.com/492228019 • https://crbug.com/492213293 • https://crbug.com/490118036 • https://crbug.com/496205576 • https://crbug.com/495931147 • https://crbug.com/495507390 • https://crbug.com/494644471 • https://crbug.com/493900619 • https://crbug.com/492139412 • https://crbug.com/493952652 • https://crbug.com/492131521

- https://crbug.com/491655161
- https://crbug.com/491518608
- https://crbug.com/491515787
- https://crbug.com/490642836
- https://crbug.com/490254128
- https://crbug.com/489791424
- https://crbug.com/489711638
- https://crbug.com/489494022
- https://crbug.com/488596746
- https://crbug.com/491732188