НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-03-16.1 | 16 марта 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-3915	Microsoft Edge	Сетевой	ACE	2026-03-14	✓
2	Высокая	CVE-2026-3931	Microsoft Edge	Сетевой	ACE	2026-03-14	✓
3	Высокая	CVE-2026-3914	Microsoft Edge	Сетевой	ACE	2026-03-14	✓
4	Высокая	CVE-2026-3924	Microsoft Edge	Сетевой	ACE	2026-03-14	✓
5	Высокая	CVE-2026-3926	Microsoft Edge	Сетевой	OSI	2026-03-14	✓
6	Высокая	CVE-2026-3920	Microsoft Edge	Сетевой	ACE	2026-03-14	✓
7	Высокая	CVE-2026-3910	Microsoft Edge	Сетевой	OSI	2026-03-14	✓
8	Высокая	CVE-2026-3919	Microsoft Edge	Сетевой	ACE	2026-03-14	✓
9	Высокая	CVE-2026-3936	Microsoft Edge	Сетевой	OSI	2026-03-14	✓
10	Высокая	CVE-2026-3918	Microsoft Edge	Сетевой	ACE	2026-03-14	✓
11	Высокая	CVE-2026-3913	Microsoft Edge	Сетевой	ACE	2026-03-14	✓
12	Критическая	CVE-2026-3916	Microsoft Edge	Сетевой	OSI	2026-03-14	✓
13	Высокая	CVE-2026-3921	Microsoft Edge	Сетевой	ACE	2026-03-14	✓

14	Высокая	CVE-2026-3923	Microsoft Edge	Сетевой	ACE	2026-03-14	✓
15	Высокая	CVE-2026-3922	Microsoft Edge	Сетевой	ACE	2026-03-14	✓
16	Высокая	CVE-2026-3917	Microsoft Edge	Сетевой	ACE	2026-03-14	✓
17	Высокая	CVE-2026-3537	Microsoft Edge	Сетевой	ACE	2026-03-14	✓
18	Высокая	CVE-2026-3909	Google Chrome	Сетевой	ACE	2026-03-14	✓
19	Высокая	CVE-2023-43010	WebKitGTK+GTK+ and WPE WebKit	Сетевой	ACE	2026-03-12	✓
20	Высокая	CVE-2026-3926	Google Chrome	Сетевой	OSI	2026-03-12	✓
21	Высокая	CVE-2026-3924	Google Chrome	Сетевой	ACE	2026-03-12	✓
22	Высокая	CVE-2026-3923	Google Chrome	Сетевой	ACE	2026-03-12	✓
23	Высокая	CVE-2026-3922	Google Chrome	Сетевой	ACE	2026-03-12	✓
24	Высокая	CVE-2026-3921	Google Chrome	Сетевой	ACE	2026-03-12	✓
25	Высокая	CVE-2026-3919	Google Chrome	Сетевой	ACE	2026-03-12	✓
26	Высокая	CVE-2026-3918	Google Chrome	Сетевой	ACE	2026-03-12	✓
27	Высокая	CVE-2026-3917	Google Chrome	Сетевой	ACE	2026-03-12	✓
28	Критическая	CVE-2026-3916	Google Chrome	Сетевой	OSI	2026-03-12	✓

29	Высокая	CVE-2026-3915	Google Chrome	Сетевой	ACE	2026-03-12	✓
30	Высокая	CVE-2026-3914	Google Chrome	Сетевой	ACE	2026-03-12	✓
31	Высокая	CVE-2026-3920	Google Chrome	Сетевой	ACE	2026-03-12	✓
32	Высокая	CVE-2026-3913	Google Chrome	Сетевой	ACE	2026-03-12	✓
33	Высокая	CVE-2026-3931	Google Chrome	Сетевой	ACE	2026-03-12	✓
34	Высокая	CVE-2026-3936	Google Chrome	Сетевой	OSI	2026-03-12	✓
35	Высокая	CVE-2026-28691	ImageMagick	Сетевой	DoS	2026-03-11	✓
36	Высокая	CVE-2026-28693	ImageMagick	Сетевой	ACE	2026-03-11	✓
37	Высокая	CVE-2026-23654	Microsoft GitHub: Zero Shot SCFoundation	Сетевой	ACE	2026-03-11	✓
38	Высокая	CVE-2026-3288	Ingress-NGINX Controller for Kubernetes	Сетевой	ACE	2026-03-11	✓
39	Высокая	CVE-2026-27269	Adobe Premiere Pro	Локальный	ACE	2026-03-11	✓
40	Высокая	CVE-2026-27280	Adobe DNG Software Development Kit	Локальный	ACE	2026-03-11	✓
41	Высокая	CVE-2026-27279	Adobe Substance 3D Stager	Локальный	ACE	2026-03-11	✓
42	Высокая	CVE-2026-27277	Adobe Substance 3D Stager	Локальный	ACE	2026-03-11	✓
43	Высокая	CVE-2026-27276	Adobe Substance 3D Stager	Локальный	ACE	2026-03-11	✓

44	Высокая	CVE-2026-27275	Adobe Substance 3D Stager	Локальный	ACE	2026-03-11	✓
45	Высокая	CVE-2026-27274	Adobe Substance 3D Stager	Локальный	ACE	2026-03-11	✓
46	Высокая	CVE-2026-27273	Adobe Substance 3D Stager	Локальный	ACE	2026-03-11	✓
47	Высокая	CVE-2026-26134	Microsoft Office	Локальный	PE	2026-03-11	✓
48	Высокая	CVE-2026-26113	Microsoft Office	Локальный	ACE	2026-03-11	✓
49	Высокая	CVE-2026-26110	Microsoft Office	Локальный	ACE	2026-03-11	✓
50	Высокая	CVE-2026-27267	Adobe Illustrator	Локальный	ACE	2026-03-11	✓
51	Высокая	CVE-2026-27272	Adobe Illustrator	Локальный	ACE	2026-03-11	✓
52	Высокая	CVE-2026-27271	Adobe Illustrator	Локальный	ACE	2026-03-11	✓
53	Высокая	CVE-2026-21362	Adobe Illustrator	Локальный	ACE	2026-03-11	✓
54	Высокая	CVE-2026-21333	Adobe Illustrator	Локальный	ACE	2026-03-11	✓
55	Высокая	CVE-2026-26144	Microsoft Excel	Сетевой	XSS\CSS	2026-03-11	✓
56	Высокая	CVE-2026-26109	Microsoft Excel	Локальный	OSI	2026-03-11	✓
57	Высокая	CVE-2026-26108	Microsoft Excel	Локальный	ACE	2026-03-11	✓
58	Высокая	CVE-2026-26107	Microsoft Excel	Локальный	ACE	2026-03-11	✓

59	Высокая	CVE-2026-26112	Microsoft Excel	Локальный	ACE	2026-03-11	✓
60	Высокая	CVE-2026-25190	Microsoft GDI	Локальный	ACE	2026-03-10	✓
61	Высокая	CVE-2026-27278	Adobe Acrobat and Reader	Локальный	ACE	2026-03-10	✓
62	Высокая	CVE-2026-27220	Adobe Acrobat and Reader	Локальный	ACE	2026-03-10	✓
63	Высокая	CVE-2026-22627	FortiSwitch AX	Смежная сеть	ACE	2026-03-10	✓
64	Высокая	CVE-2025-54820	FortiManager gtupdates service	Сетевой	ACE	2026-03-10	✓
65	Высокая	CVE-2026-24017	FortiWeb	Сетевой	ACE	2026-03-10	✓
66	Высокая	CVE-2026-25173	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2026-03-10	✓
67	Высокая	CVE-2026-25172	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2026-03-10	✓
68	Высокая	CVE-2026-26111	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2026-03-10	✓
69	Высокая	CVE-2026-3847	Mozilla Firefox	Сетевой	ACE	2026-03-10	✓
70	Высокая	CVE-2026-3845	Mozilla Firefox	Сетевой	ACE	2026-03-10	✓
71	Критическая	CVE-2026-30903	Zoom Workplace for Windows Mail feature	Сетевой	OSI	2026-03-10	✓
72	Высокая	CVE-2026-3094	Delta Electronics CNCSoft-G2	Локальный	ACE	2026-03-09	✓

73	Критическая	CVE-2026-3545	Microsoft Edge	Сетевой	ACE	2026-03-09	✓
74	Высокая	CVE-2026-3544	Microsoft Edge	Сетевой	ACE	2026-03-09	✓
75	Высокая	CVE-2026-3542	Microsoft Edge	Сетевой	OSI	2026-03-09	✓
76	Высокая	CVE-2026-3540	Microsoft Edge	Сетевой	OSI	2026-03-09	✓
77	Высокая	CVE-2026-3536	Microsoft Edge	Сетевой	ACE	2026-03-09	✓
78	Высокая	CVE-2026-3538	Microsoft Edge	Сетевой	ACE	2026-03-09	✓
79	Высокая	CVE-2026-3543	Microsoft Edge	Сетевой	OSI	2026-03-09	✓
80	Высокая	CVE-2026-3541	Microsoft Edge	Сетевой	OSI	2026-03-09	✓
81	Высокая	CVE-2026-3539	Microsoft Edge	Сетевой	ACE	2026-03-09	✓
82	Критическая	CVE-2026-20131	Cisco Secure Firewall Management Center and Cisco FTD	Сетевой	ACE	2026-03-06	✓
83	Критическая	CVE-2026-3545	Google Chrome	Сетевой	ACE	2026-03-05	✓
84	Высокая	CVE-2026-3544	Google Chrome	Сетевой	ACE	2026-03-05	✓
85	Высокая	CVE-2026-3543	Google Chrome	Сетевой	OSI	2026-03-05	✓
86	Высокая	CVE-2026-3542	Google Chrome	Сетевой	OSI	2026-03-05	✓
87	Высокая	CVE-2026-3541	Google Chrome	Сетевой	OSI	2026-03-05	✓

88	Высокая	CVE-2026-3540	Google Chrome	Сетевой	OSI	2026-03-05	✓
89	Высокая	CVE-2026-3539	Google Chrome	Сетевой	ACE	2026-03-05	✓
90	Высокая	CVE-2026-3538	Google Chrome	Сетевой	ACE	2026-03-05	✓
91	Высокая	CVE-2026-3537	Google Chrome	Сетевой	ACE	2026-03-05	✓
92	Высокая	CVE-2026-3536	Google Chrome	Сетевой	ACE	2026-03-05	✓
93	Критическая	CVE-2026-20079	Cisco Secure Firewall Management Center	Сетевой	ACE	2026-03-04	✓
94	Высокая	CVE-2025-61732	Go programming language	Локальный	ACE	2026-03-03	✓
95	Критическая	CVE-2025-68121	Go programming language	Сетевой	OSI	2026-03-03	✓
96	Высокая	CVE-2026-20048	Cisco Nexus 9000 Series Fabric Switches in ACI Mode SNMP	Сетевой	DoS	2026-02-26	✓

1

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3915

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

2	**Краткое описание:** Выполнение произвольного кода в Microsoft Edge **Идентификатор уязвимости:** CVE-2026-3931 **Идентификатор программной ошибки:** CWE-787 Запись за границами буфера **Уязвимый продукт:** Microsoft Edge: 100.0.1185.29 - 145.0.3800.99 **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:** 2026-03-14 / 2026-03-14 **Ссылки на источник:** • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913 • https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

3

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3914

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

4

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3924

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3926

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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

5

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

6

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3920

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

7

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3910

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

8

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3919

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3936

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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

9

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

10

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3918

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3913

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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

11

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

12

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3916

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 9.6 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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3921

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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

13

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

14

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3923

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

15

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3922

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

16

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3917

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.99

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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3941
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3934
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3917
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3925
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3922
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3923
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3942
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3921
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3930
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3916
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3913
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3918

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3936
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3932
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3919
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3910
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3920
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3926
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3940
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3924
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3935
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3937
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3939
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3914
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3928
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3931
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3929
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3938
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3927
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3915

17

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3537

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.97

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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3537

18

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3909

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.76

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: 2026-03-14 / 2026-03-14

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_13.html
- https://crbug.com/491421267

19

Краткое описание: Выполнение произвольного кода в WebKitGTK+GTK+ and WPE WebKit

Идентификатор уязвимости: CVE-2023-43010

Идентификатор программной ошибки: Не определено

Уязвимый продукт: WebKitGTK+: все версии
WPE WebKit: все версии

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: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://support.apple.com/en-us/126646

20

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-3926

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

21

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3924

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3923

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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

22

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

23

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3922

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3921

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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

24

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3919

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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

25

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3918

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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

26

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

27

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3917

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

28

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-3916

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 9.6 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: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

29

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3915

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3914

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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

30

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3920

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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

31

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3913

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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

32

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3931

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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

33

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

34

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-3936

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 146.0.7680.66

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: 2026-03-12 / 2026-03-12

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop_10.html
- https://crbug.com/476898368
- https://crbug.com/475238879
- https://crbug.com/474670215
- https://crbug.com/470574526
- https://crbug.com/40058077
- https://crbug.com/474763968
- https://crbug.com/473118648
- https://crbug.com/481920229
- https://crbug.com/479326680
- https://crbug.com/478783560
- https://crbug.com/478296121

- https://crbug.com/417599694
- https://crbug.com/477180001
- https://crbug.com/483445078
- https://crbug.com/482875307
- https://crbug.com/481776048
- https://crbug.com/483971526
- https://crbug.com/482828615
- https://crbug.com/483569512
- https://crbug.com/483853103
- https://crbug.com/444176961
- https://crbug.com/484946544
- https://crbug.com/435980394
- https://crbug.com/485397139
- https://crbug.com/485935314
- https://crbug.com/487338366
- https://crbug.com/418214610
- https://crbug.com/478659010
- https://crbug.com/474948986

Краткое описание: Отказ в обслуживании в ImageMagick

Идентификатор уязвимости: CVE-2026-28691

Идентификатор программной ошибки: CWE-252 Отсутствует проверка возвращаемых значений

Уязвимый продукт: ImageMagick: 6.9.13-0 - 7.1.2-15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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

35

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-56jp-jfqg-f8f4
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-r39q-jr8h-gcq2
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-qpg4-j99f-8xcg
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-hffp-q43q-qq76
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-mrmj-x24c-wwcv
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-wj8w-pjxf-9g4f
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-7h7q-j33q-hvpf
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-493f-jh8w-qhx3
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-467j-76j7-5885
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-932h-jw47-73jm
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-5ggv-92r5-cp4p

Краткое описание: Выполнение произвольного кода в ImageMagick

Идентификатор уязвимости: CVE-2026-28693

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: ImageMagick: 6.9.13-0 - 7.1.2-15

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

36

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-56jp-jfqg-f8f4
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-r39q-jr8h-gcq2
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-qpg4-j99f-8xcg
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-hffp-q43q-qq76
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-mrmj-x24c-wwcv
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-wj8w-pjxf-9g4f
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-7h7q-j33q-hvpf
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-493f-jh8w-qhx3
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-467j-76j7-5885
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-932h-jw47-73jm
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-5ggv-92r5-cp4p

37

Краткое описание: Выполнение произвольного кода в Microsoft GitHub: Zero Shot SCFoundation

Идентификатор уязвимости: CVE-2026-23654

Идентификатор программной ошибки: Не определено

Уязвимый продукт: GitHub Repo: Zero Shot scFoundation: до 0.1.1

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: 8.8 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: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-23654

38

Краткое описание: Выполнение произвольного кода в Ingress-NGINX Controller for Kubernetes

Идентификатор уязвимости: CVE-2026-3288

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Ingress-NGINX Controller for Kubernetes: 1.0.0 - 1.14.3

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: 8.8 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: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://github.com/kubernetes/kubernetes/issues/137560
- http://www.openwall.com/lists/oss-security/2026/03/09/8

39

Краткое описание: Выполнение произвольного кода в Adobe Premiere Pro

Идентификатор уязвимости: CVE-2026-27269

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Premiere Pro: 22.0 - 25.5

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/premiere_pro/apsb26-28.html

40

Краткое описание: Выполнение произвольного кода в Adobe DNG Software Development Kit

Идентификатор уязвимости: CVE-2026-27280

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe DNG Software Development Kit (SDK): 1.7.0 - 1.7.1.2471

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/dng-sdk/apsb26-30.html

41

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2026-27279

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Stager: 3.0.2 - 3.1.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-29.html

42

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2026-27277

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Substance 3D Stager: 3.0.2 - 3.1.7

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: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-29.html

43

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2026-27276

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Substance 3D Stager: 3.0.2 - 3.1.7

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: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-29.html

44

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2026-27275

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Stager: 3.0.2 - 3.1.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-29.html

45

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2026-27274

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Stager: 3.0.2 - 3.1.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-29.html

46

Краткое описание: Выполнение произвольного кода в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2026-27273

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Stager: 3.0.2 - 3.1.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-29.html

47

Краткое описание: Повышение привилегий в Microsoft Office

Идентификатор уязвимости: CVE-2026-26134

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

Уязвимый продукт: Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Office: до 16.0.5543.1000
Microsoft Office for Android: до 16.0.19822.20000
Microsoft SharePoint Server: до 16.0.10417.20102
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20076
Microsoft SharePoint Enterprise Server: до 16.0.5543.1000

Категория уязвимого продукта: Операционные системы Microsoft 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.

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: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26110
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26113
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26134

48

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-26113

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Office: до 16.0.5543.1000
Microsoft Office for Android: до 16.0.19822.20000
Microsoft SharePoint Server: до 16.0.10417.20102
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20076
Microsoft SharePoint Enterprise Server: до 16.0.5543.1000

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.4 AV:L/AC:L/PR:N/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: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26110
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26113
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26134

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-26110

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

Уязвимый продукт: Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Office: до 16.0.5543.1000
Microsoft Office for Android: до 16.0.19822.20000
Microsoft SharePoint Server: до 16.0.10417.20102
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20076
Microsoft SharePoint Enterprise Server: до 16.0.5543.1000

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

49

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: 8.4 AV:L/AC:L/PR:N/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: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26110
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26113
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26134

50

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2026-27267

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Adobe Illustrator: 22.0 - 30.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/illustrator/apsb26-18.html

51

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2026-27272

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Illustrator: 22.0 - 30.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/illustrator/apsb26-18.html

52

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2026-27271

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

Уязвимый продукт: Adobe Illustrator: 22.0 - 30.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/illustrator/apsb26-18.html

53

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2026-21362

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Illustrator: 22.0 - 30.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/illustrator/apsb26-18.html

54

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2026-21333

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Adobe Illustrator: 22.0 - 30.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/illustrator/apsb26-18.html

Краткое описание: Межсайтовый скриптинг в Microsoft Excel

Идентификатор уязвимости: CVE-2026-26144

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

Уязвимый продукт: Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Excel: до 16.0.5543.1000
Office Online Server : до 16.0.10417.20102

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: Межсайтовый скриптинг

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

Оценка CVSSv3: 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: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26112
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26107
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26108
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26109
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26144

56

Краткое описание: Получение конфиденциальной информации в Microsoft Excel

Идентификатор уязвимости: CVE-2026-26109

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Excel: до 16.0.5543.1000
Office Online Server : до 16.0.10417.20102

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Чтение за пределами буфера.

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: 8.4 AV:L/AC:L/PR:N/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: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26112
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26107
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26108
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26109
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26144

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-26108

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

Уязвимый продукт: Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Excel: до 16.0.5543.1000
Office Online Server : до 16.0.10417.20102

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.

57

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: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26112
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26107
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26108
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26109
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26144

58

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-26107

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Excel: до 16.0.5543.1000
Office Online Server : до 16.0.10417.20102

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26112
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26107
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26108
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26109
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26144

59

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-26112

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024 for Mac
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems
Microsoft Excel: до 16.0.5543.1000
Office Online Server : до 16.0.10417.20102

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: 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: 2026-03-11 / 2026-03-11

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26112
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26107
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26108
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26109
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26144

60

Краткое описание: Выполнение произвольного кода в Microsoft GDI

Идентификатор уязвимости: CVE-2026-25190

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Windows: 10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.7840
Windows Server: 2012 6.2.9200.24768 - 2025 10.0.26100.32370

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: 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: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-25190

61

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2026-27278

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 2025.011.2
Adobe Reader: 20.001.30002 - 25.001.21265

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: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-26.html

62

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2026-27220

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Acrobat: 15.006.30306 - 2025.011.2
Adobe Reader: 20.001.30002 - 25.001.21265

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: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb26-26.html

Краткое описание: Выполнение произвольного кода в FortiSwitch AX

Идентификатор уязвимости: CVE-2026-22627

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

Уязвимый продукт: FortiSwitch AX: 1.0.0 - 1.0.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

63 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-26-085
- https://www.fortiguard.com/psirt/FG-IR-26-086

64

Краткое описание: Выполнение произвольного кода в FortiManager gtupdates service

Идентификатор уязвимости: CVE-2025-54820
BDU:2026-02878

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: FortiManager: 6.4.0 - 7.4.2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных 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: 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: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-26-098
- https://bdu.fstec.ru/vul/2026-02878

65

Краткое описание: Выполнение произвольного кода в FortiWeb

Идентификатор уязвимости: CVE-2026-24017

Идентификатор программной ошибки: CWE-799 Некорректное ограничение частоты взаимодействия

Уязвимый продукт: FortiWeb: 7.0.0 - 8.0.2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных 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: 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: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-26-082

66

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2026-25173

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

Уязвимый продукт: Windows Server: 2012 6.2.9200.24768 - 2025 10.0.26100.32370
Windows: 10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.7840

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Подключение к вредоносному серверу.

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: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26111
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-25172
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-25173

67

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2026-25172

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

Уязвимый продукт: Windows Server: 2012 6.2.9200.24768 - 2025 10.0.26100.32370
Windows: 10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.7840

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка пользователем запроса к вредоносному серверу

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: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26111
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-25172
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-25173

68

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2026-26111

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

Уязвимый продукт: Windows Server: 2012 6.2.9200.24768 - 2025 10.0.26100.32370
Windows: 10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.7840

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка пользователем запроса к вредоносному серверу

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: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26111
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-25172
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-25173

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2026-3847

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

Уязвимый продукт: Firefox for Android: 141.0 - 148.0.1
Mozilla Firefox: 141.0 - 148.0

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.

69

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: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-19/
- https://bugzilla.mozilla.org/show_bug.cgi?id=2020174
- https://bugzilla.mozilla.org/show_bug.cgi?id=2018400
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=2017513
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=2017622
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=2019341

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2026-3845

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

Уязвимый продукт: Firefox for Android: 141.0 - 148.0.1
Mozilla Firefox: 141.0 - 148.0

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.

70

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: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-19/
- https://bugzilla.mozilla.org/show_bug.cgi?id=2020174
- https://bugzilla.mozilla.org/show_bug.cgi?id=2018400
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=2017513
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=2017622
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=2019341

71

Краткое описание: Получение конфиденциальной информации в Zoom Workplace for Windows Mail feature

Идентификатор уязвимости: CVE-2026-30903

Идентификатор программной ошибки: CWE-73 Внешнее управление именем или путем файла

Уязвимый продукт: Zoom Workplace Desktop App for Windows: 0.9.10042.0911 - 6.5.12 14128
Virtual Desktop Infrastructure (VDI): 6.4.10.26150 - 6.5.14.26880

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 9.6 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: 2026-03-10 / 2026-03-10

Ссылки на источник:

- https://www.zoom.com/en/trust/security-bulletin/ZSB-26005/

72

Краткое описание: Выполнение произвольного кода в Delta Electronics CNCSoft-G2

Идентификатор уязвимости: CVE-2026-3094

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: CNCSoft-G2: до 2.1.0.39

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-09 / 2026-03-09

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-26-151/https://www.cisa.gov/news-events/ics-advisories/icsa-26-064-01

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3545

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.82

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

73 **Оценка CVSSv4:** Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-09 / 2026-03-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3539
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3541
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3543
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3538
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3536
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3540
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3542
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3544
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3545

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3544

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.82

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

74 **Оценка CVSSv4:** Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-09 / 2026-03-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3539
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3541
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3543
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3538
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3536
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3540
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3542
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3544
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3545

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3542

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.82

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

75 **Оценка CVSSv4:** Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-09 / 2026-03-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3539
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3541
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3543
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3538
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3536
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3540
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3542
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3544
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3545

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3540

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.82

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

76 **Оценка CVSSv4:** Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-09 / 2026-03-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3539
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3541
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3543
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3538
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3536
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3540
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3542
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3544
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3545

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3536

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.82

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

77 **Оценка CVSSv4:** Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-09 / 2026-03-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3539
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3541
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3543
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3538
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3536
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3540
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3542
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3544
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3545

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3538

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

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.82

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

78 **Оценка CVSSv4:** Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-09 / 2026-03-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3539
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3541
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3543
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3538
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3536
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3540
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3542
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3544
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3545

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3543

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.82

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

79 **Оценка CVSSv4:** Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-09 / 2026-03-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3539
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3541
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3543
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3538
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3536
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3540
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3542
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3544
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3545

Краткое описание: Получение конфиденциальной информации в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3541

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.82

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

80 **Оценка CVSSv4:** Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-09 / 2026-03-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3539
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3541
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3543
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3538
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3536
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3540
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3542
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3544
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3545

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2026-3539

Идентификатор программной ошибки: CWE-1091 Использование объекта без последующего вызова деструктора

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 145.0.3800.82

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

81 **Оценка CVSSv4:** Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-09 / 2026-03-09

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3539
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3541
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3543
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3538
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3536
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3540
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3542
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3544
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-3545

82

Краткое описание: Выполнение произвольного кода в Cisco Secure Firewall Management Center and Cisco FTD

Идентификатор уязвимости: CVE-2026-20131

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Cisco Secure Firewall Management Center (formerly Firepower Management Center, FMC): 6.4.0.13 - 10.0.0
Cisco Firewall Threat Defense (FTD): 6.4.0.13 - 10.0.0

Категория уязвимого продукта: Средства защиты информации

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-03-06 / 2026-03-06

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwt14636

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3545

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.119

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

83

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-05 / 2026-03-05

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop.html
- https://issues.chromium.org/issues/485622239
- https://issues.chromium.org/issues/474266014
- https://crbug.com/484983991
- https://crbug.com/483853098
- https://crbug.com/484088917
- https://crbug.com/484811719
- https://crbug.com/485152421
- https://crbug.com/485267831
- https://crbug.com/485683110
- https://crbug.com/487383169

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3544

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.119

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

84

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-05 / 2026-03-05

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop.html
- https://issues.chromium.org/issues/485622239
- https://issues.chromium.org/issues/474266014
- https://crbug.com/484983991
- https://crbug.com/483853098
- https://crbug.com/484088917
- https://crbug.com/484811719
- https://crbug.com/485152421
- https://crbug.com/485267831
- https://crbug.com/485683110
- https://crbug.com/487383169

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-3543

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.119

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

85

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-05 / 2026-03-05

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop.html
- https://issues.chromium.org/issues/485622239
- https://issues.chromium.org/issues/474266014
- https://crbug.com/484983991
- https://crbug.com/483853098
- https://crbug.com/484088917
- https://crbug.com/484811719
- https://crbug.com/485152421
- https://crbug.com/485267831
- https://crbug.com/485683110
- https://crbug.com/487383169

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-3542

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.119

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

86

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-05 / 2026-03-05

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop.html
- https://issues.chromium.org/issues/485622239
- https://issues.chromium.org/issues/474266014
- https://crbug.com/484983991
- https://crbug.com/483853098
- https://crbug.com/484088917
- https://crbug.com/484811719
- https://crbug.com/485152421
- https://crbug.com/485267831
- https://crbug.com/485683110
- https://crbug.com/487383169

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-3541

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.119

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

87

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-05 / 2026-03-05

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop.html
- https://issues.chromium.org/issues/485622239
- https://issues.chromium.org/issues/474266014
- https://crbug.com/484983991
- https://crbug.com/483853098
- https://crbug.com/484088917
- https://crbug.com/484811719
- https://crbug.com/485152421
- https://crbug.com/485267831
- https://crbug.com/485683110
- https://crbug.com/487383169

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2026-3540

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.119

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

88

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-05 / 2026-03-05

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop.html
- https://issues.chromium.org/issues/485622239
- https://issues.chromium.org/issues/474266014
- https://crbug.com/484983991
- https://crbug.com/483853098
- https://crbug.com/484088917
- https://crbug.com/484811719
- https://crbug.com/485152421
- https://crbug.com/485267831
- https://crbug.com/485683110
- https://crbug.com/487383169

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3539

Идентификатор программной ошибки: CWE-1091 Использование объекта без последующего вызова деструктора

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.119

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

89

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-05 / 2026-03-05

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop.html
- https://issues.chromium.org/issues/485622239
- https://issues.chromium.org/issues/474266014
- https://crbug.com/484983991
- https://crbug.com/483853098
- https://crbug.com/484088917
- https://crbug.com/484811719
- https://crbug.com/485152421
- https://crbug.com/485267831
- https://crbug.com/485683110
- https://crbug.com/487383169

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3538

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.119

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

90

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-05 / 2026-03-05

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop.html
- https://issues.chromium.org/issues/485622239
- https://issues.chromium.org/issues/474266014
- https://crbug.com/484983991
- https://crbug.com/483853098
- https://crbug.com/484088917
- https://crbug.com/484811719
- https://crbug.com/485152421
- https://crbug.com/485267831
- https://crbug.com/485683110
- https://crbug.com/487383169

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3537

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.119

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

91

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-05 / 2026-03-05

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop.html
- https://issues.chromium.org/issues/485622239
- https://issues.chromium.org/issues/474266014
- https://crbug.com/484983991
- https://crbug.com/483853098
- https://crbug.com/484088917
- https://crbug.com/484811719
- https://crbug.com/485152421
- https://crbug.com/485267831
- https://crbug.com/485683110
- https://crbug.com/487383169

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-3536

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 145.0.7632.119

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

92

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-03-05 / 2026-03-05

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/03/stable-channel-update-for-desktop.html
- https://issues.chromium.org/issues/485622239
- https://issues.chromium.org/issues/474266014
- https://crbug.com/484983991
- https://crbug.com/483853098
- https://crbug.com/484088917
- https://crbug.com/484811719
- https://crbug.com/485152421
- https://crbug.com/485267831
- https://crbug.com/485683110
- https://crbug.com/487383169

93

Краткое описание: Выполнение произвольного кода в Cisco Secure Firewall Management Center

Идентификатор уязвимости: CVE-2026-20079

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

Уязвимый продукт: Cisco Secure Firewall Management Center (formerly Firepower Management Center, FMC): 7.0.0 - 7.7.11

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса 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: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwr96008

94

Краткое описание: Выполнение произвольного кода в Go programming language

Идентификатор уязвимости: CVE-2025-61732

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

Уязвимый продукт: Go programming language: 1.24 rc1 - 1.25.6

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://groups.google.com/g/golang-announce/c/K09ubi9FQFk?pli=1

95

Краткое описание: Получение конфиденциальной информации в Go programming language

Идентификатор уязвимости: CVE-2025-68121

Идентификатор программной ошибки: CWE-295 Некорректная проверка сертификатов

Уязвимый продукт: Go programming language: 1.24 rc1 - 1.25.6

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Некорректная проверка сертификатов.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://groups.google.com/g/golang-announce/c/K09ubi9FQFk?pli=1

96

Краткое описание: Отказ в обслуживании в Cisco Nexus 9000 Series Fabric Switches in ACI Mode SNMP

Идентификатор уязвимости: CVE-2026-20048

Идентификатор программной ошибки: CWE-789 Неконтролируемое выделение памяти

Уязвимый продукт: Cisco NX-OS: до 16.1(5e)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.7 AV:N/AC:L/PR:L/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: 2026-02-26 / 2026-02-26

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-dsnmp-cNN39Uhhttps://bst.cloudapps.cisco.com/bugsearch/bug/CSCwq57598