НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-09-09.1 | 9 сентября 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	**Критическая**	CVE-2026-9967	Google Chrome	Сетевой	DoS	2026-08-03	✔️
2	**Высокая**	CVE-2026-9965	Google Chrome	Сетевой	DoS	2026-08-03	✔️
3	**Высокая**	CVE-2026-9962	Google Chrome	Сетевой	DoS	2026-08-03	✔️
4	**Высокая**	CVE-2026-9961	Google Chrome	Сетевой	DoS	2026-08-03	✔️
5	**Высокая**	CVE-2026-9960	Google Chrome	Сетевой	DoS	2026-08-03	✔️
6	**Высокая**	CVE-2026-9958	Google Chrome	Сетевой	DoS	2026-08-03	✔️
7	**Высокая**	CVE-2026-9957	Google Chrome	Сетевой	DoS	2026-08-03	✔️
8	**Высокая**	CVE-2026-9954	Google Chrome	Сетевой	DoS	2026-08-03	✔️
9	**Высокая**	CVE-2026-9952	Google Chrome	Сетевой	DoS	2026-08-03	✔️
10	**Высокая**	CVE-2026-9951	Google Chrome	Сетевой	DoS	2026-08-03	✔️

11	**Высокая**	CVE-2026-9968	Google Chrome	Сетевой	DoS	2026-08-03	✔️
12	**Высокая**	CVE-2026-9947	Google Chrome	Сетевой	DoS	2026-08-03	✔️
13	**Высокая**	CVE-2026-9941	Google Chrome	Сетевой	DoS	2026-08-03	✔️
14	**Высокая**	CVE-2026-9940	Google Chrome	Сетевой	DoS	2026-08-03	✔️
15	**Высокая**	CVE-2026-9939	Google Chrome	Сетевой	DoS	2026-08-03	✔️
16	**Высокая**	CVE-2026-9938	Google Chrome	Сетевой	DoS	2026-08-03	✔️
17	**Высокая**	CVE-2026-9934	Google Chrome	Сетевой	DoS	2026-08-03	✔️
18	**Высокая**	CVE-2026-9933	Google Chrome	Сетевой	DoS	2026-08-03	✔️
19	**Высокая**	CVE-2026-9931	Google Chrome	Сетевой	DoS	2026-08-03	✔️
20	**Высокая**	CVE-2026-9927	Google Chrome	Сетевой	DoS	2026-08-03	✔️
21	**Высокая**	CVE-2026-9926	Google Chrome	Сетевой	DoS	2026-08-03	✔️
22	**Высокая**	CVE-2026-9925	Google Chrome	Сетевой	DoS	2026-08-03	✔️

23	**Высокая**	CVE-2026-9946	Google Chrome	Сетевой	DoS	2026-08-03	✔️
24	**Высокая**	CVE-2026-9969	Google Chrome	Сетевой	DoS	2026-08-03	✔️
25	**Высокая**	CVE-2026-9970	Google Chrome	Сетевой	DoS	2026-08-03	✔️
26	**Высокая**	CVE-2026-9974	Google Chrome	Сетевой	DoS	2026-08-03	✔️
27	**Высокая**	CVE-2026-13281	Google Chrome	Сетевой	DoS	2026-08-03	✔️
28	**Высокая**	CVE-2026-9119	Google Chrome	Сетевой	DoS	2026-08-03	✔️
29	**Высокая**	CVE-2026-9126	Google Chrome	Сетевой	DoS	2026-08-03	✔️
30	**Высокая**	CVE-2026-9121	Google Chrome	Сетевой	DoS	2026-08-03	✔️
31	**Высокая**	CVE-2026-9120	Google Chrome	Сетевой	DoS	2026-08-03	✔️
32	**Высокая**	CVE-2026-9117	Google Chrome	Сетевой	DoS	2026-08-03	✔️
33	**Высокая**	CVE-2026-9114	Google Chrome	Сетевой	DoS	2026-08-03	✔️
34	**Высокая**	CVE-2026-9111	Google Chrome	Сетевой	DoS	2026-08-03	✔️

35	Высокая	CVE-2026-9123	Google Chrome	Смежная сеть	DoS	2026-08-03	✔️
36	Высокая	CVE-2026-8587	Google Chrome	Сетевой	ACE	2026-08-06	✔️
37	Высокая	CVE-2026-8585	Google Chrome	Сетевой	SB	2026-08-06	✔️
38	Критическая	CVE-2026-8580	Google Chrome	Сетевой	DoS	2026-08-03	✔️
39	Высокая	CVE-2026-8577	Google Chrome	Сетевой	DoS	2026-08-03	✔️
40	Высокая	CVE-2026-9997	Google Chrome	Сетевой	DoS	2026-08-03	✔️
41	Высокая	CVE-2026-9995	Google Chrome	Сетевой	DoS	2026-08-03	✔️
42	Высокая	CVE-2026-9993	Google Chrome	Сетевой	DoS	2026-08-03	✔️
43	Высокая	CVE-2026-9992	Google Chrome	Сетевой	DoS	2026-08-03	✔️
44	Высокая	CVE-2026-9988	Google Chrome	Сетевой	DoS	2026-08-03	✔️
45	Высокая	CVE-2026-9983	Google Chrome	Сетевой	DoS	2026-08-03	✔️
46	Высокая	CVE-2026-9982	Google Chrome	Сетевой	DoS	2026-08-03	✔️

47	Высокая	CVE-2026-9978	Google Chrome	Сетевой	DoS	2026-08-03	✔️
48	Высокая	CVE-2026-9976	Google Chrome	Сетевой	DoS	2026-08-03	✔️
49	Высокая	CVE-2026-9975	Google Chrome	Сетевой	DoS	2026-08-03	✔️
50	Высокая	CVE-2026-9923	Google Chrome	Сетевой	DoS	2026-08-03	✔️
51	Критическая	CVE-2026-9918	Google Chrome	Сетевой	DoS	2026-08-03	✔️
52	Высокая	CVE-2026-8581	Google Chrome	Сетевой	DoS	2026-08-03	✔️
53	Высокая	CVE-2026-9915	Google Chrome	Сетевой	DoS	2026-08-03	✔️
54	Высокая	CVE-2026-43233	Linux	Сетевой	DoS	2026-07-29	✔️
55	Высокая	CVE-2026-43232	Linux	Сетевой	ACE	2026-07-28	✔️
56	Высокая	CVE-2026-43230	Linux	Сетевой	DoS	2026-07-28	✔️
57	Высокая	CVE-2026-43214	Linux	Локальный	ACE	2026-07-28	✔️
58	Высокая	CVE-2026-43211	Linux	Локальный	ACE	2026-07-28	✔️

59	**Высокая**	CVE-2026-43207	Linux	Локальный	ACE	2026-07-28	✔️
60	**Высокая**	CVE-2026-43206	Linux	Локальный	ACE	2026-07-28	✔️
61	**Высокая**	CVE-2026-43203	Linux	Сетевой	ACE	2026-07-28	✔️
62	**Высокая**	CVE-2026-43196	Linux	Локальный	ACE	2026-07-28	✔️
63	**Высокая**	CVE-2026-43190	Linux	Сетевой	DoS	2026-07-29	✔️
64	**Критическая**	CVE-2026-43186	Linux	Сетевой	ACE	2026-07-27	✔️
65	**Высокая**	CVE-2026-43150	Linux	Локальный	ACE	2026-07-28	✔️
66	**Высокая**	CVE-2026-43139	Linux	Сетевой	ACE	2026-07-28	✔️
67	**Высокая**	CVE-2026-43133	Linux	Локальный	ACE	2026-07-28	✔️
68	**Высокая**	CVE-2026-23156	Linux	Локальный	ACE	2026-08-05	✔️
69	**Высокая**	CVE-2026-23112	Linux	Смежная сеть	ACE	2026-07-28	✔️
70	**Высокая**	CVE-2026-23098	Linux	Смежная сеть	ACE	2026-08-05	✔️

71	Высокая	CVE-2026-23089	Linux	Локальный	ACE	2026-08-04	✔
72	Высокая	CVE-2026-23078	Linux	Локальный	ACE	2026-08-04	✔
73	Высокая	CVE-2026-23073	Linux	Локальный	ACE	2026-08-04	✔
74	Высокая	CVE-2026-23068	Linux	Локальный	ACE	2026-08-04	✔
75	Высокая	CVE-2026-9916	Google Chrome	Сетевой	DoS	2026-08-03	✔
76	Высокая	CVE-2026-43236	Linux	Локальный	ACE	2026-07-28	✔
77	Высокая	CVE-2026-43304	Linux	Сетевой	ACE	2026-07-28	✔
78	Критическая	CVE-2026-9874	Google Chrome	Сетевой	DoS	2026-08-03	✔
79	Высокая	CVE-2026-9914	Google Chrome	Сетевой	DoS	2026-08-03	✔
80	Критическая	CVE-2026-63077	TeamCity	Сетевой	SB	2026-08-06	✔
81	Критическая	CVE-2026-54917	SeaweedFS	Сетевой	ACE	2026-08-06	✔
82	Высокая	CVE-2026-69250	Flowise	Сетевой	RLF	2026-08-05	✔

83	**Высокая**	CVE-2026-9910	Google Chrome	Сетевой	DoS	2026-08-03	✔️
84	**Высокая**	CVE-2026-9909	Google Chrome	Сетевой	DoS	2026-08-03	✔️
85	**Высокая**	CVE-2026-9906	Google Chrome	Сетевой	DoS	2026-08-03	✔️
86	**Высокая**	CVE-2026-9904	Google Chrome	Сетевой	DoS	2026-08-03	✔️
87	**Высокая**	CVE-2026-9902	Google Chrome	Сетевой	DoS	2026-08-03	✔️
88	**Высокая**	CVE-2026-9900	Google Chrome	Сетевой	DoS	2026-08-03	✔️
89	**Высокая**	CVE-2026-9899	Google Chrome	Сетевой	DoS	2026-08-03	✔️
90	**Высокая**	CVE-2026-9873	Google Chrome	Сетевой	DoS	2026-08-03	✔️
91	**Высокая**	CVE-2026-9901	Google Chrome	Сетевой	DoS	2026-08-03	✔️
92	**Высокая**	CVE-2026-9895	Google Chrome	Сетевой	DoS	2026-08-03	✔️
93	**Высокая**	CVE-2026-9877	Google Chrome	Сетевой	DoS	2026-08-03	✔️
94	**Высокая**	CVE-2026-9878	Google Chrome	Сетевой	DoS	2026-08-03	✔️

95	Высокая	CVE-2026-9897	Google Chrome	Сетевой	DoS	2026-08-03	✔
96	Высокая	CVE-2026-9880	Google Chrome	Сетевой	DoS	2026-08-03	✔
97	Высокая	CVE-2026-9883	Google Chrome	Сетевой	DoS	2026-08-03	✔
98	Высокая	CVE-2026-9879	Google Chrome	Сетевой	DoS	2026-08-03	✔
99	Критическая	CVE-2026-9891	Google Chrome	Сетевой	DoS	2026-08-03	✔
100	Высокая	CVE-2026-9893	Google Chrome	Сетевой	DoS	2026-08-03	✔
101	Высокая	CVE-2026-9894	Google Chrome	Сетевой	DoS	2026-08-03	✔
102	Высокая	CVE-2026-9896	Google Chrome	Сетевой	DoS	2026-08-03	✔
103	Высокая	CVE-2026-9887	Google Chrome	Сетевой	DoS	2026-08-03	✔
104	Критическая	CVE-2026-20304	Cisco SD-WAN	Сетевой	ACE	2026-08-06	✔
105	Высокая	CVE-2026-20124	Cisco IOS XE	Сетевой	DoS	2026-08-07	✔
106	Высокая	CVE-2026-20301	Cisco IOS XE	Сетевой	DoS	2026-08-06	✔

107	Критическая	CVE-2026-20267	Cisco IOS XE	Сетевой	ACE	2026-08-06	✔️
108	Критическая	CVE-2026-20303	Cisco SD-WAN	Сетевой	ACE	2026-08-06	✔️
109	Критическая	CVE-2026-20310	Cisco SD-WAN	Сетевой	ACE	2026-08-06	✔️
110	Высокая	CVE-2026-20273	Cisco IOS XE	Сетевой	DoS	2026-08-06	✔️
111	Высокая	CVE-2026-20200	Integrated Management Controller	Сетевой	PE	2026-08-07	✔️
112	Высокая	CVE-2026-20270	Cisco IOS XE	Сетевой	DoS	2026-08-06	✔️
113	Высокая	CVE-2026-20269	Cisco IOS XE	Сетевой	DoS	2026-08-06	✔️
114	Критическая	CVE-2026-20272	Cisco IOS XE	Сетевой	ACE	2026-08-06	✔️
115	Высокая	CVE-2026-20268	Cisco IOS XE	Сетевой	DoS	2026-08-06	✔️
116	Высокая	CVE-2026-70601	Electron	Сетевой	ACE	2026-08-06	✔️
117	Высокая	CVE-2026-20271	Cisco IOS XE	Сетевой	DoS	2026-08-06	✔️
118	Высокая	CVE-2026-55723	NGINX Ingress Controller	Сетевой	DoS	2026-07-16	✔️

119	Высокая	CVE-2026-20296	Splunk Enterprise	Сетевой	ACE	2026-07-16	✔️
120	Высокая	CVE-2026-31432	Linux	Сетевой	ACE	2026-08-07	✔️
121	Критическая	CVE-2026-43341	Linux	Сетевой	ACE	2026-07-27	✔️
122	Критическая	CVE-2026-59309	VMware vCenter Server	Сетевой	OSI	2026-07-30	✔️
123	Критическая	CVE-2026-59310	VMware vCenter Server	Сетевой	ACE	2026-07-30	✔️
124	Критическая	CVE-2026-47876	VMware ESXi	Локальный	ACE	2026-07-30	✔️
125	Высокая	CVE-2026-43084	Linux	Локальный	ACE	2026-08-10	✔️
126	Высокая	CVE-2026-43334	Linux	Смежная сеть	ACE	2026-08-10	✔️
127	Критическая	CVE-2026-31444	Linux	Сетевой	ACE	2026-08-07	✔️
128	Высокая	CVE-2026-46129	Linux	Локальный	ACE	2026-08-10	✔️
129	Критическая	CVE-2026-46119	Linux	Сетевой	OAF	2026-08-10	✔️
130	Критическая	CVE-2026-46155	Linux	Сетевой	OAF	2026-08-10	✔️

1

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9967
BDU:2026-11172

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9967
- https://security-tracker.debian.org/tracker/CVE-2026-9967
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/506414791
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-11172

2

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9965
BDU:2026-11171

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9965
- https://security-tracker.debian.org/tracker/CVE-2026-9965
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/506377574
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9965
- https://bdu.fstec.ru/vul/2026-11171

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9962
BDU:2026-11170

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

3

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9962
- https://security-tracker.debian.org/tracker/CVE-2026-9962
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/504716948
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9962
- https://bdu.fstec.ru/vul/2026-11170

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9961
BDU:2026-11169

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

4

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9961
- https://security-tracker.debian.org/tracker/CVE-2026-9961
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/504710769
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9961
- https://bdu.fstec.ru/vul/2026-11169

5

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9960
BDU:2026-11168

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9960
- https://security-tracker.debian.org/tracker/CVE-2026-9960
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/504573260
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9960
- https://bdu.fstec.ru/vul/2026-11168

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9958
BDU:2026-11167

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

6

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9958
- https://security-tracker.debian.org/tracker/CVE-2026-9958
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/504555886
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9958
- https://bdu.fstec.ru/vul/2026-11167

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9957
BDU:2026-11166

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

7

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9957
- https://security-tracker.debian.org/tracker/CVE-2026-9957
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/504516117
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9957
- https://bdu.fstec.ru/vul/2026-11166

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9954
BDU:2026-11165

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

8

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9954
- https://security-tracker.debian.org/tracker/CVE-2026-9954
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/504175497
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9954
- https://bdu.fstec.ru/vul/2026-11165

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9952
BDU:2026-11163

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

9

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9952
- https://security-tracker.debian.org/tracker/CVE-2026-9952
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/503929476
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9952
- https://bdu.fstec.ru/vul/2026-11163

10

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9951
BDU:2026-11162

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9951
- https://security-tracker.debian.org/tracker/CVE-2026-9951
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/503873388
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9951
- https://bdu.fstec.ru/vul/2026-11162

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9968
BDU:2026-11173

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9968
- https://security-tracker.debian.org/tracker/CVE-2026-9968
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/506499280
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9968
- https://bdu.fstec.ru/vul/2026-11173

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9947
BDU:2026-11161

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9947
- https://security-tracker.debian.org/tracker/CVE-2026-9947
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/503627446
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9947
- https://bdu.fstec.ru/vul/2026-11161

1
2

13

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9941
BDU:2026-11157

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9941
- https://security-tracker.debian.org/tracker/CVE-2026-9941
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/502812366
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9941
- https://bdu.fstec.ru/vul/2026-11157

14

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9940
BDU:2026-11156

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9940
- https://security-tracker.debian.org/tracker/CVE-2026-9940
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/502738003
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9940
- https://bdu.fstec.ru/vul/2026-11156

15

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9939
BDU:2026-11155

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9939
- https://security-tracker.debian.org/tracker/CVE-2026-9939
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/502735235
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9939
- https://bdu.fstec.ru/vul/2026-11155

16

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9938
BDU:2026-11154

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9938
- https://security-tracker.debian.org/tracker/CVE-2026-9938
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/502300817
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9938
- https://bdu.fstec.ru/vul/2026-11154

17

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9934
BDU:2026-11152

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9934
- https://security-tracker.debian.org/tracker/CVE-2026-9934
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/501576946
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9934
- https://bdu.fstec.ru/vul/2026-11152

18

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9933
BDU:2026-11151

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9933
- https://security-tracker.debian.org/tracker/CVE-2026-9933
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/501575979
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9933
- https://bdu.fstec.ru/vul/2026-11151

19

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9931
BDU:2026-11150

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9931
- https://security-tracker.debian.org/tracker/CVE-2026-9931
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/501524262
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9931
- https://bdu.fstec.ru/vul/2026-11150

20

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9927
BDU:2026-11149

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9927
- https://security-tracker.debian.org/tracker/CVE-2026-9927
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/500540958
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9927
- https://bdu.fstec.ru/vul/2026-11149

21

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9926
BDU:2026-11148

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9926
- https://security-tracker.debian.org/tracker/CVE-2026-9926
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/500540748
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9926
- https://bdu.fstec.ru/vul/2026-11148

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9925
BDU:2026-11147

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

2
2

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9925
- https://security-tracker.debian.org/tracker/CVE-2026-9925
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/500536458
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9925
- https://bdu.fstec.ru/vul/2026-11147

23

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9946
BDU:2026-11160

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9946
- https://security-tracker.debian.org/tracker/CVE-2026-9946
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/503596863
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9946
- https://bdu.fstec.ru/vul/2026-11160

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9969
BDU:2026-11174

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

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.

2 4

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9969
- https://security-tracker.debian.org/tracker/CVE-2026-9969
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/506550494
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9969
- https://bdu.fstec.ru/vul/2026-11174

25

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9970
BDU:2026-11175

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9970
- https://security-tracker.debian.org/tracker/CVE-2026-9970
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/506653647
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9970
- https://bdu.fstec.ru/vul/2026-11175

26

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9974
BDU:2026-11176

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9974
- https://security-tracker.debian.org/tracker/CVE-2026-9974
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/511710468
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9974
- https://bdu.fstec.ru/vul/2026-11176

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-13281
BDU:2026-11215

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

Уязвимый продукт: Google Chrome: до 149.0.7827.201
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-13281
- https://security-tracker.debian.org/tracker/CVE-2026-13281
- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_01245939337.html
- https://issues.chromium.org/issues/513138301
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-11215

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9119
BDU:2026-11214

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

Уязвимый продукт: Google Chrome: до 148.0.7778.179
Microsoft Edge: до 148.0.3967.83
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

28

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9119
- https://security-tracker.debian.org/tracker/CVE-2026-9119
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0841193308.html
- https://issues.chromium.org/issues/502661101
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://redos.red-soft.ru/support/secure/uyazvimosti/uyazvimost-chromium-cve-2026-9119-7.3/?sphrase_id=1557766
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-chromium-cve-2026-9119-8.0/?sphrase_id=1557766

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9119
- https://bdu.fstec.ru/vul/2026-11214

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9126
BDU:2026-11213

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.179
Microsoft Edge: до 148.0.3967.83
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9126
- https://security-tracker.debian.org/tracker/CVE-2026-9126
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0841193308.html
- https://issues.chromium.org/issues/496280532
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF

- https://redos.red-soft.ru/support/secure/uyazvimosti/uyazvimost-chromium-cve-2026-9126-7.3/?sphrase_id=1557783
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-chromium-cve-2026-9126-8.0/?sphrase_id=1557783
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9126
- https://bdu.fstec.ru/vul/2026-11213

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9121
BDU:2026-11211

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.179
Microsoft Edge: до 148.0.3967.83
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9121
- https://security-tracker.debian.org/tracker/CVE-2026-9121
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0841193308.html

- https://issues.chromium.org/issues/488064108
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://redos.red-soft.ru/support/secure/uyazvimosti/uyazvimost-chromium-cve-2026-9121-7.3/?sphrase_id=1557771
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-chromium-cve-2026-9121-8.0/?sphrase_id=1557771
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9121
- https://bdu.fstec.ru/vul/2026-11211

3 1

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9120
BDU:2026-11210

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.179
Microsoft Edge: до 148.0.3967.83
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9120

- https://security-tracker.debian.org/tracker/CVE-2026-9120
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0841193308.html
- https://issues.chromium.org/issues/504620824
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://redos.red-soft.ru/support/secure/uyazvimosti/uyazvimost-chromium-cve-2026-9120-7.3/?sphrase_id=1557770
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-chromium-cve-2026-9120-8.0/?sphrase_id=1557770
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9120
- https://bdu.fstec.ru/vul/2026-11210

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9117
BDU:2026-11209

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

Уязвимый продукт: Google Chrome: до 148.0.7778.179
Microsoft Edge: до 148.0.3967.83
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-03 / 2026-08-03

3
2

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9117
- https://security-tracker.debian.org/tracker/CVE-2026-9117
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0841193308.html
- https://issues.chromium.org/issues/497542537
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://redos.red-soft.ru/support/secure/uyazvimosti/uyazvimost-chromium-cve-2026-9117-7.3/?sphrase_id=1557758
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-chromium-cve-2026-9117-8.0/?sphrase_id=1557758
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9117
- https://bdu.fstec.ru/vul/2026-11209

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9114
BDU:2026-11206

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.179
Microsoft Edge: до 148.0.3967.83
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

33 **Категория уязвимого продукта:** Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9114
- https://security-tracker.debian.org/tracker/CVE-2026-9114
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0841193308.html
- https://issues.chromium.org/issues/495798630
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://redos.red-soft.ru/support/secure/uyazvimosti/uyazvimost-chromium-cve-2026-9114-7.3/?sphrase_id=1557712
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-chromium-cve-2026-9114-8.0/?sphrase_id=1557712
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9114
- https://bdu.fstec.ru/vul/2026-11206

34

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9111
BDU:2026-11205

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.179
Microsoft Edge: до 148.0.3967.83
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9111
- https://security-tracker.debian.org/tracker/CVE-2026-9111
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0841193308.html
- https://issues.chromium.org/issues/504551032
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://redos.red-soft.ru/support/secure/uyazvimosti/uyazvimost-chromium-cve-2026-9111-7.3/?sphrase_id=1557528
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-chromium-cve-2026-9111-8.0/?sphrase_id=1557528
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9111
- https://bdu.fstec.ru/vul/2026-11205

35

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9123
BDU:2026-11204

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

Уязвимый продукт: Google Chrome: до 148.0.7778.179
Microsoft Edge: до 148.0.3967.83
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 AV:A/AC:H/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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9123
- https://security-tracker.debian.org/tracker/CVE-2026-9123
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0841193308.html
- https://issues.chromium.org/issues/495988507
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9123
- https://bdu.fstec.ru/vul/2026-11204

36

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-8587
BDU:2026-11202

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-gqc5-p594-9chj
- https://issues.Google Chrome.org/issues/507356235
- https://nvd.nist.gov/vuln/detail/CVE-2026-8587
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8587
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8587
- https://security-tracker.debian.org/tracker/CVE-2026-8587
- https://bdu.fstec.ru/vul/2026-11202

37

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-8585
BDU:2026-11200

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://github.com/advisories/GHSA-jwm6-pr74-mmpq
- https://issues.Google Chrome.org/issues/499052720
- https://nvd.nist.gov/vuln/detail/CVE-2026-8585
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-8585
- https://security-tracker.debian.org/tracker/CVE-2026-8585
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8585
- https://bdu.fstec.ru/vul/2026-11200

38

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-8580
BDU:2026-11196

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8580
- https://security-tracker.debian.org/tracker/CVE-2026-8580
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://issues.chromium.org/issues/496639647
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://redos.red-soft.ru/support/secure/uyazvimosti/uyazvimost-chromium-cve-2026-8580-7.3/?sphrase_id=1557518
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-chromium-cve-2026-8580-8.0/?sphrase_id=1557518
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8580
- https://bdu.fstec.ru/vul/2026-11196

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-8577
BDU:2026-11193

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

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8577
- https://security-tracker.debian.org/tracker/CVE-2026-8577
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://issues.chromium.org/issues/496302307
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://redos.red-soft.ru/support/secure/uyazvimosti/uyazvimost-chromium-cve-2026-8577-7.3/?sphrase_id=1557512
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-chromium-cve-2026-8577-8.0/?sphrase_id=1557512
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8577
- https://bdu.fstec.ru/vul/2026-11193

40

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9997
BDU:2026-11191

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления

программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9997
- https://security-tracker.debian.org/tracker/CVE-2026-9997
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513324041
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://github.com/George0Papasotiriou/CVE-2026-9997-VPN-Split-Tunneling-Bypass-via-DHCP-Option-Injection
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9997
- https://bdu.fstec.ru/vul/2026-11191

41

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9995
BDU:2026-11190

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления

программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9995
- https://security-tracker.debian.org/tracker/CVE-2026-9995
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513256572
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9995
- https://bdu.fstec.ru/vul/2026-11190

42

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9993
BDU:2026-11189

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9993
- https://security-tracker.debian.org/tracker/CVE-2026-9993
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513208588
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9993
- https://bdu.fstec.ru/vul/2026-11189

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9992
BDU:2026-11188

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

43

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9992
- https://security-tracker.debian.org/tracker/CVE-2026-9992
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513177826
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9992
- https://bdu.fstec.ru/vul/2026-11188

4 4

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9988
BDU:2026-11186

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9988
- https://security-tracker.debian.org/tracker/CVE-2026-9988
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513049286
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9988
- https://bdu.fstec.ru/vul/2026-11186

4 5

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9983
BDU:2026-11184

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9983
- https://security-tracker.debian.org/tracker/CVE-2026-9983
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513001309
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9983
- https://bdu.fstec.ru/vul/2026-11184

46

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9982
BDU:2026-11183

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9982
- https://security-tracker.debian.org/tracker/CVE-2026-9982
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513001247
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9982
- https://bdu.fstec.ru/vul/2026-11183

47

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9978
BDU:2026-11179

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9978
- https://security-tracker.debian.org/tracker/CVE-2026-9978
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/511741396
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9978
- https://bdu.fstec.ru/vul/2026-11179

48

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9976
BDU:2026-11178

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9976
- https://security-tracker.debian.org/tracker/CVE-2026-9976
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/511732828
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9976
- https://bdu.fstec.ru/vul/2026-11178

49

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9975
BDU:2026-11177

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9975
- https://security-tracker.debian.org/tracker/CVE-2026-9975
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/511719039
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9975
- https://bdu.fstec.ru/vul/2026-11177

50

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9923
BDU:2026-11146

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9923
- https://security-tracker.debian.org/tracker/CVE-2026-9923
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/500393328
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9923
- https://bdu.fstec.ru/vul/2026-11146

5 1

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9918
BDU:2026-11145

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 9.6 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9918
- https://security-tracker.debian.org/tracker/CVE-2026-9918
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/500099471
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9918
- https://bdu.fstec.ru/vul/2026-11145

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-8581
BDU:2026-11197

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.167
Microsoft Edge: до 148.0.3967.70
Debian GNU/Linux: 13
РЕД ОС: 8.0
Astra Linux Special Edition: 1.8

5
2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-8581
- https://security-tracker.debian.org/tracker/CVE-2026-8581
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_12.html
- https://issues.chromium.org/issues/497292072
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://redos.red-soft.ru/support/secure/uyazvimosti/uyazvimost-chromium-cve-2026-8581-7.3/?sphrase_id=1557522
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-chromium-cve-2026-8581-8.0/?sphrase_id=1557522
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-8581
- https://bdu.fstec.ru/vul/2026-11197

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9915
BDU:2026-11143

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

5
3

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9915
- https://security-tracker.debian.org/tracker/CVE-2026-9915
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/500063836
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9915
- https://bdu.fstec.ru/vul/2026-11143

54

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43233
BDU:2026-11101

Идентификатор программной ошибки: CWE-131 Некорректный расчет размера буфера

Уязвимый продукт: Linux: от 4.15 до 5.10.251 включительно
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43233
- https://git.kernel.org/stable/c/bcb50aa0b8f2b74a9fe5a1c7bee6f2657a288041
- https://git.kernel.org/stable/c/2a3aac4205e7d2f1aca2e3827de8cdd517d36c4a
- https://git.kernel.org/stable/c/81f2fc5b0d0cf4696146f00f837596d10b92dead
- https://git.kernel.org/stable/c/7ef82863d42261817a6394c6c881bd6757a70f16
- https://git.kernel.org/stable/c/53d32735d77ab56cc3fc7bd53a7d099418f19be1
- https://git.kernel.org/stable/c/f0a83d0a4b7c127d32ac06d607a9214937716129
- https://git.kernel.org/stable/c/35f1943d242e1b9f0b6e91c0c93bfb293a9f8224
- https://git.kernel.org/linus/baed0d9ba91d4f390da12d5039128ee897253d60
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11101

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43232
BDU:2026-11100

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.1.2 до 6.1.164 включительно
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://git.kernel.org/stable/c/cac048ebfbb92d91d719f74b59177cb70a7633b8
- https://www.cve.org/CVERecord?id=CVE-2026-43232
- https://git.kernel.org/stable/c/086131807d119238cd464e5b0845e48d938dfd79
- https://git.kernel.org/stable/c/ae894e47e1cd5a6bf8a0423d888c45df8b2b02dc
- https://git.kernel.org/stable/c/337d7b4112a47984ee319171b75b73bab47e7924
- https://git.kernel.org/stable/c/200bdb8d367ca9b478f9c56ebe56411604d55c81
- https://git.kernel.org/stable/c/21d341fe514fd07e345ed264c9eee21cb2061ca2
- https://git.kernel.org/stable/c/04edfdfdfcdefc02408ab670607261b0a0a9a02e
- https://git.kernel.org/linus/bae8a5d2e759da2e0cba33ab2080deee96a09373
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11100

5 6

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43230
BDU:2026-11099

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

Уязвимый продукт: Linux: от 2.6.30 до 5.10.251 включительно
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://git.kernel.org/stable/c/3cf001aff71b1db1b4732a5381b012a114720664
- https://git.kernel.org/stable/c/60b347333ec259ac7352f62cbbc365b04c065ff8
- https://git.kernel.org/stable/c/597c46a42930c963f448720aaf5001dd4ed98af4
- https://git.kernel.org/stable/c/391200c274e90c34071b909ba12e3390b81b767f
- https://git.kernel.org/stable/c/ba2e3472022f44baddf000621fed150d7a599ea3
- https://git.kernel.org/stable/c/14eae5564053ac3973b9369dc674638f22f4765e
- https://git.kernel.org/stable/c/bcf034fa5f66b6a3e787f765a917934a2045cf7a
- https://www.cve.org/CVERecord?id=CVE-2026-43230
- https://git.kernel.org/linus/b89fc7c2523b2b0750d91840f4e52521270d70ed
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11099

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43214
BDU:2026-11098

Идентификатор программной ошибки: CWE-820 Отсутствие синхронизации

Уязвимый продукт: Linux: от 5.14 до 6.1.164 включительно
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

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

Оценка CVSSv4: Не определено

5
7

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43214
- https://git.kernel.org/stable/c/f621ca24f9f489e226e22560761b04884984133b
- https://git.kernel.org/stable/c/708e20c66b2761d878a2bc3c7534e7f814e4dec5
- https://git.kernel.org/stable/c/9f2bfea51151dfbb24b52f452eb3d5f5fe0e506e
- https://git.kernel.org/stable/c/57536ff0a6bd69a5808d682925202babdb5ddc13
- https://git.kernel.org/stable/c/b33f8d816950b10e7879cd8ffd7ae4b649ada4db
- https://git.kernel.org/linus/95d848dc7e639988dbb385a8cba9b484607cf98c
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11098

58

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43211
BDU:2026-11097

Идентификатор программной ошибки: CWE-832 Разблокировка незаблокированного ресурса

Уязвимый продукт: Linux: от 6.10.10 до 6.12.74 включительно
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43211
- https://git.kernel.org/stable/c/ebb27b7399ab8b9eb1f792b329aa5f6250c590d4
- https://git.kernel.org/stable/c/fbe06a3058114bf95a17a4941b205f4b321c6f0a
- https://git.kernel.org/stable/c/943ed56606a7ab2fe5a99cad572dd17d484310c7
- https://git.kernel.org/stable/c/a19b61fdb958ffadbba85b43c991eb9fc70c1c1c
- https://git.kernel.org/stable/c/0425aaf20b407d2f2cf3bf469808e4a35f9abb8b
- https://git.kernel.org/stable/c/bd435f4b738130d732ef64e0e57e45185f77165d
- https://git.kernel.org/stable/c/8b08ea9690b212b7bf7f12414039259cf34b1aa0
- https://git.kernel.org/linus/9368d1ee62829b08aa31836b3ca003803caf0b72
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11097

59

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43207
BDU:2026-11096

Идентификатор программной ошибки: CWE-567 Несинхронизированный доступ к общим данным в многопоточном контексте

Уязвимый продукт: Linux: от 4.10 до 5.10.251 включительно
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование сроками и состоянием.

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: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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://git.kernel.org/stable/c/2e8f53a7382943411557e370f1a4f3946624a30e
- https://www.cve.org/CVERecord?id=CVE-2026-43207
- https://git.kernel.org/stable/c/9d9c67976eda502edc6b3a148a1c5b6a18b69a98
- https://git.kernel.org/stable/c/0bc43eaf021347f8d5aba87712c36b799695eec6
- https://git.kernel.org/stable/c/9d7962d5c81d6cf3f8dbdb5c71c57600bac5772b
- https://git.kernel.org/stable/c/12cafc15d24611bfb43c82877b1bbb7454a85d5a
- https://git.kernel.org/stable/c/c8737d33d4e8ffae87e5d5edac17f8a705235cc2
- https://git.kernel.org/stable/c/b3fc99fe5b25613dd61c57bc70b8479adff4f60d
- https://git.kernel.org/linus/8a8a3232abac5b972058a5f2cb3e33199d2a8648
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11096

60

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43206
BDU:2026-11095

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 4.17 до 5.10.251 включительно
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся

обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43206
- https://git.kernel.org/stable/c/3e04bc310d80b46eaf481f1fefcbcb37a187412d
- https://git.kernel.org/stable/c/de8d7a25cd2eb5875b1d8d4fbc7fe4b4138b781f
- https://git.kernel.org/stable/c/b4034442cb090e4a980bdcc1540948606cbc951b
- https://git.kernel.org/stable/c/4857c37c7ba9aa38b9a4c694e8bd8d0091c87940
- https://git.kernel.org/stable/c/75fb57efdd7863fffbc39db23e9cad7aafda26ed
- https://git.kernel.org/stable/c/bfcd6b53e1f4feb182952f4ff9a137c36ceaf20b
- https://git.kernel.org/linus/8a70a26c9f34baea6c3199a9862ddaff4554a96d
- https://git.kernel.org/stable/c/4e72f419e4ed44cb3b60506752d8688c20a60a9b
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11095

6 1

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43203
BDU:2026-11094

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 2.6.12 до 5.10.251 включительно
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43203
- https://git.kernel.org/stable/c/91f25749aaf57c47ae1e12478144e6ea8c8562f2
- https://git.kernel.org/stable/c/73fbc5d1a9ccb626937500bbd67136f077d8237b
- https://git.kernel.org/stable/c/aba0b4bc09376dfc3d53c826514fe38fc8337f52
- https://git.kernel.org/stable/c/e075ec9b08f862dade8011481058f7eb5f716c57
- https://git.kernel.org/stable/c/97900f512252a59f23d6ce4ab215cc88fed66e68
- https://git.kernel.org/stable/c/e4ff4e3ffcf9d5aad380cdd1d8cdc008bb34f97d
- https://git.kernel.org/stable/c/5189368f10903956be05062d160b2804bf5e5016
- https://git.kernel.org/linus/8930878101cd40063888a68af73b1b0f8b6c79bc
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11094

62

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43196
BDU:2026-11093

Идентификатор программной ошибки: CWE-1074 Класс со слишком глубоким наследованием

Уязвимый продукт: Linux: от 5.11 до 5.15.201 включительно
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43196
- https://git.kernel.org/stable/c/dbda01bf2dfe5af33163e1e5fca1b82b619c2803
- https://git.kernel.org/stable/c/24c40076e3bc3d73c839c886d6bda1da6c4d9b93
- https://git.kernel.org/stable/c/818cf66d91c8ef09b01664a12d5f4ea786d64396
- https://git.kernel.org/stable/c/e113339cc7d23be4948891f3a702e9dce5b47035
- https://git.kernel.org/stable/c/69aa67c1e22d13e9aad4b08c86304ad8e743dcab
- https://git.kernel.org/stable/c/b7db9953c2f8da37de498198623b05b46f8e2ca0
- https://git.kernel.org/stable/c/04dbbb18cc9c8795c9ff47d8994bc03ebfef9d68
- https://git.kernel.org/linus/80db65d4acfb9ff12d00172aed39ea8b98261aad
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11093

63

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43190
BDU:2026-11092

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

Уязвимый продукт: Linux: от 2.6.12 до 5.10.251 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions

Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.2 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-29 / 2026-07-29

Ссылки на источник:

- https://git.kernel.org/stable/c/f895191dc32c53eaf443b6443fe40945b2f92287
- https://git.kernel.org/stable/c/cd5beda7e0e32865e214f28034bb92c1cecff885
- https://git.kernel.org/stable/c/eaedc0bc18be46fe7f58170e967959a932c4f824
- https://git.kernel.org/stable/c/07a9b32eaae792ff7d0fcac14d8920c937c0a9c3
- https://git.kernel.org/stable/c/8b300f726640c48c3edfe9c453334dd801f4b74e
- https://git.kernel.org/stable/c/5e13d0a37666955b6cfddc0f73cb40ed645b8a05
- https://git.kernel.org/stable/c/f6c412dcfd76b0516d51aa847d8f4c7b70381b09
- https://git.kernel.org/linus/735ee8582da3d239eb0c7a53adca61b79fb228b3
- https://www.cve.org/CVERecord?id=CVE-2026-43190
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://security-tracker.debian.org/tracker/CVE-2026-43190
- https://ubuntu.com/security/CVE-2026-43190
- https://access.redhat.com/security/cve/cve-2026-43190
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11092

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43186
BDU:2026-11091

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.7 до 6.12.74 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

64

Оценка CVSSv3: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43186
- https://git.kernel.org/stable/c/fb3c662fafebc5b9d74417ed1de8759f6bb72143
- https://git.kernel.org/stable/c/632d233cf2e64a46865ae2c064ae3c9df7c8864f
- https://git.kernel.org/stable/c/e90346a2f1e8917d5760a44a1f61c44e3b36d96b
- https://git.kernel.org/stable/c/ea3632aefc04205436868541638e26f4a74d5637
- https://git.kernel.org/linus/6db8b56eed62baacaf37486e83378a72635c04cc
- https://git.kernel.org/stable/c/f4d9d4b8fd839719d564651671e24c62c545c23b

- https://git.kernel.org/stable/c/0591d6509c2ff13f09ea2998434aba0c0472e978
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://security-tracker.debian.org/tracker/CVE-2026-43186
- https://ubuntu.com/security/CVE-2026-43186
- https://access.redhat.com/security/cve/cve-2026-43186
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11091

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43150
BDU:2026-11090

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.5 до 6.6.127 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-28 / 2026-07-28

Ссылки на источник:

65

- https://www.cve.org/CVERecord?id=CVE-2026-43150
- https://git.kernel.org/stable/c/7e2c200010aa93fa78201da959b4ac6b9f8fed0b
- https://git.kernel.org/stable/c/d3e837e11ee9ed08df229272319199003ba00379
- https://git.kernel.org/stable/c/00d69f21ef2ab00e6156c764d89e2b3539eb2f33
- https://git.kernel.org/stable/c/08c7eadd8a934a1968e1aeeee8b61b853b99fb3a
- https://git.kernel.org/stable/c/a251d866f50b6a4c95901fa722025065679c2eca
- https://git.kernel.org/linus/36c0de02575ce59dfd879eb4ef63d53a68bbf9ce
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://security-tracker.debian.org/tracker/CVE-2026-43150
- https://ubuntu.com/security/CVE-2026-43150
- https://access.redhat.com/security/cve/cve-2026-43150
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11090

6 6

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43139
BDU:2026-11088

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Linux: от 2.6.19 до 5.10.251 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43139
- https://git.kernel.org/stable/c/4f28141786e1fe884ce42a5197ba9beed540f0ea
- https://git.kernel.org/stable/c/6535867673bf301d52aa00593a4d1d18cc3922fa
- https://git.kernel.org/stable/c/eb2ee15290af14c60b45cf2b73f5687d1d077d9b
- https://git.kernel.org/stable/c/719918fc88df6da023dfff370cd965151a5afd7f
- https://git.kernel.org/stable/c/dc0abce055134cb83b0d981d31ceb20dda419787
- https://git.kernel.org/stable/c/c7221e7bd8fc2ef38a0b27be580d9d202281306b
- https://git.kernel.org/stable/c/3dcd1664ac15eee6a690daec7c4ffc59190406f7
- https://git.kernel.org/linus/1799d8abeabc68ec05679292aaf6cba93b343c05
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://security-tracker.debian.org/tracker/CVE-2026-43139
- https://ubuntu.com/security/CVE-2026-43139
- https://access.redhat.com/security/cve/cve-2026-43139
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11088

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43133
BDU:2026-11087

Идентификатор программной ошибки: CWE-680 Целочисленное переполнение, приводящее к переполнению буфера

Уязвимый продукт: Linux: от 5.13 до 5.15.201 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
OpenShift Container Platform: 4
Astra Linux Special Edition: 4.8

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

6
7

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.9 AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43133
- https://git.kernel.org/stable/c/10063e1251c1485034a018236080792ad083dcc5
- https://git.kernel.org/stable/c/3880e331b0b31d0d5d3702b124f6c93539cd478a
- https://git.kernel.org/stable/c/fce2fd4a2ca05670a91015aacccf96a1c26268fd
- https://git.kernel.org/stable/c/d464cf1ed900d47c85393d40b00017b6adfc2e6c
- https://git.kernel.org/stable/c/0004ecb798b30e90d7ebfe74efae2d9423315a64
- https://git.kernel.org/linus/127ccae2c185f62e6ecb4bf24f9cb307e9b9c619
- https://git.kernel.org/stable/c/c3b7015000988ba35ecd5648f4b2283960f00543
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://access.redhat.com/security/cve/cve-2026-43133
- https://ubuntu.com/security/CVE-2026-43133
- https://security-tracker.debian.org/tracker/CVE-2026-43133
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11087

Краткое описание: Выполнение произвольного кода в Linux

6 8 **Идентификатор уязвимости:** CVE-2026-23156
BDU:2026-11080

Идентификатор программной ошибки: CWE-390 Обнаружение ошибки без реагирования на нее

Уязвимый продукт: Linux: от 6.2 до 6.6.122 включительно
Red Hat Enterprise Linux: 10.0 Extended Update Support
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://git.kernel.org/stable/c/89b8ca709eeeabcc11ebba64806677873a2787a8
- https://git.kernel.org/stable/c/e4e15a0a4403c96d9898d8398f0640421df9cb16
- https://git.kernel.org/stable/c/3960f1754664661a970dc9ebbab44ff93a0b4c42
- https://git.kernel.org/stable/c/510a16f1c5c1690b33504052bc13fbc2772c23f8
- https://www.cve.org/CVERecord?id=CVE-2026-23156
- https://git.kernel.org/linus/4b22ec1685ce1fc0d862dcda3225d852fb107995
- https://security-tracker.debian.org/tracker/CVE-2026-23156
- https://ubuntu.com/security/CVE-2026-23156
- https://access.redhat.com/security/cve/cve-2026-23156
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11080

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23112
BDU:2026-11076

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.7 до 6.12.69 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 25.10
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.6 AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-23112
- https://git.kernel.org/stable/c/043b4307a99f902697349128fde93b2ddde4686c
- https://git.kernel.org/stable/c/42afe8ed8ad2de9c19457156244ef3e1eca94b5d
- https://git.kernel.org/stable/c/1385be357e8acd09b36e026567f3a9d5c61139de
- https://git.kernel.org/stable/c/dca1a6ba0da9f472ef040525fab10fd9956db59f
- https://git.kernel.org/stable/c/19672ae68d52ff75347ebe2420dde1b07adca09f
- https://git.kernel.org/stable/c/ab200d71553bdcf4de554a5985b05b2dd606bc57

- https://git.kernel.org/linus/52a0a98549344ca20ad81a4176d68d28e3c05a5c
- https://security-tracker.debian.org/tracker/CVE-2026-23112
- https://access.redhat.com/security/cve/CVE-2026-23112
- https://ubuntu.com/security/CVE-2026-23112
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11076

70

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23098
BDU:2026-11074

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Linux: от 2.6.12 до 5.10.248 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://git.kernel.org/stable/c/25aab6bfc31017a7e52035b99aef5c2b6bde8ffb

- https://git.kernel.org/stable/c/94d1a8bd08af1f4cc345c5c29f5db1ea72b8bb8c
- https://git.kernel.org/stable/c/6e0110ea90313b7c0558a0b77038274a6821caf8
- https://git.kernel.org/stable/c/9f5fa78d9980fe75a69835521627ab7943cb3d67
- https://git.kernel.org/stable/c/bd8955337e3764f912f49b360e176d8aaecf7016
- https://git.kernel.org/stable/c/7c48fdf2d1349bb54815b56fb012b9d577707708
- https://www.cve.org/CVERecord?id=CVE-2026-23098
- https://git.kernel.org/linus/ba1096c315283ee3292765f6aea4cca15816c4f7
- https://security-tracker.debian.org/tracker/CVE-2026-23098
- https://ubuntu.com/security/CVE-2026-23098
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11074

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23089
BDU:2026-11072

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 2.6.13 до 5.10.248 включительно
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

7 1 **Категория уязвимого продукта:** Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://git.kernel.org/stable/c/dc1a5dd80af1ee1f29d8375b12dd7625f6294dad
- https://git.kernel.org/stable/c/51b1aa6fe7dc87356ba58df06afb9677c9b841ea
- https://git.kernel.org/stable/c/7bff0156d13f0ad9436e5178b979b063d59f572a
- https://git.kernel.org/stable/c/56fb6efd5d04caf6f14994d51ec85393b9a896c6
- https://git.kernel.org/stable/c/7009daeefa945973a530b2f605fe445fc03747af
- https://git.kernel.org/stable/c/e6f103a22b08daf5df2f4aa158081840e5910963
- https://www.cve.org/CVERecord?id=CVE-2026-23089
- https://git.kernel.org/linus/930e69757b74c3ae083b0c3c7419bfe7f0edc7b2
- https://security-tracker.debian.org/tracker/CVE-2026-23089
- https://access.redhat.com/security/cve/CVE-2026-23089
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11072

7 2

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23078
BDU:2026-11071

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 5.14 до 5.15.198 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся

обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков.

Оценка CVSSv3: 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: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://git.kernel.org/stable/c/91a756d22f0482eac5bedb113c8922f90b254449
- https://git.kernel.org/stable/c/51049f6e3f05d70660e2458ad3bb302a3721b751
- https://git.kernel.org/stable/c/d5e80d1f97ae55bcea1426f551e4419245b41b9c
- https://git.kernel.org/stable/c/27049f50be9f5ae3a62d272128ce0b381cb26a24
- https://git.kernel.org/stable/c/31a3eba5c265a763260976674a22851e83128f6d
- https://www.cve.org/CVERecord?id=CVE-2026-23078
- https://git.kernel.org/linus/6f5c69f72e50d51be3a8c028ae7eda42c82902cb
- https://security-tracker.debian.org/tracker/CVE-2026-23078
- https://access.redhat.com/security/cve/CVE-2026-23078
- https://ubuntu.com/security/CVE-2026-23078
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11071

7 3

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-23073
BDU:2026-11070

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 3.15 до 5.10.248 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://git.kernel.org/stable/c/7c54d0c3e2cad4300be721ec2aecfcf8a63bc9f4
- https://git.kernel.org/stable/c/49ef094fdbc3526e5db2aebb404b84f79c5603dc
- https://git.kernel.org/stable/c/99129d80a5d4989ef8566f434f3589f60f28042b
- https://git.kernel.org/stable/c/0d7c9e793e351cbbe9e06a9ca47d77b6ad288fb0
- https://git.kernel.org/stable/c/7761d7801f40e61069b4df3db88b36d80d089f8a
- https://git.kernel.org/stable/c/31efbcff90884ea5f65bf3d1de01267db51ee3d1
- https://www.cve.org/CVERecord?id=CVE-2026-23073
- https://git.kernel.org/linus/4f431d88ea8093afc7ba55edf4652978c5a68f33
- https://security-tracker.debian.org/tracker/CVE-2026-23073
- https://ubuntu.com/security/CVE-2026-23073
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11070

Краткое описание: Выполнение произвольного кода в Linux

74 **Идентификатор уязвимости:** CVE-2026-23068
BDU:2026-11069

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Linux: от 4.17 до 6.1.161 включительно
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-08-04 / 2026-08-04

Ссылки на источник:

- https://git.kernel.org/stable/c/346775f2b4cf839177e8e86b94aa180a06dc15b0
- https://git.kernel.org/stable/c/f6d6b3f172df118db582fe5ec43ae223a55d99cf
- https://git.kernel.org/stable/c/417cdfd9b9f986e95bfcb1d68eb443e6e0a15f8c
- https://git.kernel.org/stable/c/bddd3d10d039729b81cfb0804520c8832a701a0e
- https://www.cve.org/CVERecord?id=CVE-2026-23068
- https://git.kernel.org/linus/383d4f5cffcc8df930d95b06518a9d25a6d74aac
- https://security-tracker.debian.org/tracker/CVE-2026-23068
- https://ubuntu.com/security/CVE-2026-23068
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11069

7 5 **Краткое описание:** Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9916

BDU:2026-11144

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9916
- https://security-tracker.debian.org/tracker/CVE-2026-9916
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/500080303
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9916
- https://bdu.fstec.ru/vul/2026-11144

76

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43236
BDU:2026-11102

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 4.1 до 5.10.251 включительно
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43236
- https://git.kernel.org/stable/c/fd4a4d0711f48a99b25bcd45e00eef8339eff82d
- https://git.kernel.org/stable/c/6404898af86d986db1dbbe06177c143e40652e49
- https://git.kernel.org/stable/c/796e77c14c4c1e2cd36473760fb6cc66c695eb47
- https://git.kernel.org/stable/c/ac2d898da5095d46bd1ff8585fdd753d58ad91e7
- https://git.kernel.org/stable/c/a205740a7231e967ac77cb731171642901c327af
- https://git.kernel.org/stable/c/7b4d0fab3ff2c00c6d34e1952c9df5129a826aee
- https://git.kernel.org/stable/c/549c6db503dbb85dbff4840830971853feac6625
- https://git.kernel.org/linus/bc847787233277a337788568e90a6ee1557595eb
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11102

77

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43304
BDU:2026-11106

Идентификатор программной ошибки: CWE-1011 Авторизация

Уязвимый продукт: Linux: от 5.11 до 5.15.201 включительно
Astra Linux Special Edition: 4.8

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-28 / 2026-07-28

Ссылки на источник:

- https://git.kernel.org/stable/c/c1a0f5f1e5e7e98c36a362ec3d1fcfd9932931ed
- https://www.cve.org/CVERecord?id=CVE-2026-43304
- https://git.kernel.org/stable/c/6405e8c680974bb74e2c98d5249fb52c7b12a6c6
- https://git.kernel.org/stable/c/8d745d38c88ecbed95f6b2b39857bf89f35a3244
- https://git.kernel.org/stable/c/e1dc45d97975f9db65694d234fbddf1915176e16
- https://git.kernel.org/stable/c/1b275bd49e58752efb83767a5d1aed41356c5e64
- https://git.kernel.org/stable/c/d82467c07b03a27c3c5469b62bb3b726305a80bb
- https://git.kernel.org/linus/ac431d597a9bdfc2ba6b314813f29a6ef2b4a3bf
- https://wiki.astralinux.ru/astra-linux-se38-bulletin-2026-0729SE38
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0806SE48
- https://bdu.fstec.ru/vul/2026-11106

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9874
BDU:2026-11110

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9874
- https://security-tracker.debian.org/tracker/CVE-2026-9874
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/500609038
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-9874
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9874
- https://bdu.fstec.ru/vul/2026-11110

7
8

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9914
BDU:2026-11142

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

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.

7
9

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9914
- https://security-tracker.debian.org/tracker/CVE-2026-9914
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/500047428
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9914
- https://bdu.fstec.ru/vul/2026-11142

Краткое описание: Обход безопасности в TeamCity

Идентификатор уязвимости: CVE-2026-63077
BDU:2026-11140

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: TeamCity: до 2025.11.7

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Обход безопасности

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

8 0

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://www.jetbrains.com/privacy-security/issues-fixed/
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-63077
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-11140

Краткое описание: Выполнение произвольного кода в SeaweedFS

Идентификатор уязвимости: CVE-2026-54917
BDU:2026-11136

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

Уязвимый продукт: SeaweedFS: до 4.30

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://github.com/seaweedfs/seaweedfs/pull/9687
- https://github.com/seaweedfs/seaweedfs/security/advisories/GHSA-w62w-66v9-vvgv
- https://github.com/BiiTts/CVE-2026-54917-SeaweedFS-Cross-Bucket-Traversal
- https://feedly.com/cve/CVE-2026-54917
- https://bdu.fstec.ru/vul/2026-11136

Краткое описание: Чтение локальных файлов в Flowise

Идентификатор уязвимости: CVE-2026-69250
BDU:2026-11135

Идентификатор программной ошибки: CWE-639 Обход авторизации, используя значение ключа пользователя

Уязвимый продукт: Flowise: до 3.1.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Чтение локальных файлов

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

Оценка CVSSv3: 8.7 AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-05 / 2026-08-05

Ссылки на источник:

- https://github.com/FlowiseAI/Flowise/commit/da8b251a9a4c59484ceaf6f71df7406aede7bef2
- https://github.com/FlowiseAI/Flowise/releases/tag/flowise@3.1.3
- https://github.com/FlowiseAI/Flowise/security/advisories/GHSA-r745-8hwv-h473
- https://bdu.fstec.ru/vul/2026-11135

8
2

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9910
BDU:2026-11133

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

8 3

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9910
- https://security-tracker.debian.org/tracker/CVE-2026-9910
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/499176133
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9910
- https://bdu.fstec.ru/vul/2026-11133

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9909
BDU:2026-11132

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

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

8
4

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

Оценка CVSSv3: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9909
- https://security-tracker.debian.org/tracker/CVE-2026-9909
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/499152771
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://bdu.fstec.ru/vul/2026-11132

8
5

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9906
BDU:2026-11130

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9906
- https://security-tracker.debian.org/tracker/CVE-2026-9906
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/499005260
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9906
- https://bdu.fstec.ru/vul/2026-11130

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9904
BDU:2026-11129

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

8 6

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9904
- https://security-tracker.debian.org/tracker/CVE-2026-9904
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/498804020
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9904
- https://bdu.fstec.ru/vul/2026-11129

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9902
BDU:2026-11127

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

8 7

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9902
- https://security-tracker.debian.org/tracker/CVE-2026-9902
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/498205735
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9902
- https://bdu.fstec.ru/vul/2026-11127

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9900
BDU:2026-11125

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

8
8

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9900
- https://security-tracker.debian.org/tracker/CVE-2026-9900
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/497637277
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9900
- https://bdu.fstec.ru/vul/2026-11125

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9899
BDU:2026-11124

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

8 9

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9899
- https://security-tracker.debian.org/tracker/CVE-2026-9899
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/497533569
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9899
- https://bdu.fstec.ru/vul/2026-11124

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9873
BDU:2026-11109

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

9
0

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9873
- https://security-tracker.debian.org/tracker/CVE-2026-9873
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/507365348
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9873
- https://security-tracker.debian.org/tracker/CVE-2026-9873
- https://bdu.fstec.ru/vul/2026-11109

9
1

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9901
BDU:2026-11126

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9901
- https://security-tracker.debian.org/tracker/CVE-2026-9901
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/497737770
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9901
- https://bdu.fstec.ru/vul/2026-11126

9
2

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9895
BDU:2026-11122

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9895
- https://security-tracker.debian.org/tracker/CVE-2026-9895
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/491685406
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9895/
- https://bdu.fstec.ru/vul/2026-11122

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9877
BDU:2026-11111

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

9
3

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9877
- https://security-tracker.debian.org/tracker/CVE-2026-9877
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/496445460
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-9877
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9877
- https://bdu.fstec.ru/vul/2026-11111

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9878
BDU:2026-11112

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

9
4

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9878
- https://security-tracker.debian.org/tracker/CVE-2026-9878
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/499054245
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-9878
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9878
- https://bdu.fstec.ru/vul/2026-11112

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9897
BDU:2026-11123

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

9 5

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9897
- https://security-tracker.debian.org/tracker/CVE-2026-9897
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/496271580
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9897
- https://bdu.fstec.ru/vul/2026-11123

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9880
BDU:2026-11114

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

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.

9
6

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9880
- https://security-tracker.debian.org/tracker/CVE-2026-9880
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/503615025
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-9880
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9880
- https://bdu.fstec.ru/vul/2026-11114

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9883
BDU:2026-11116

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

9
7

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9883
- https://security-tracker.debian.org/tracker/CVE-2026-9883
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/506477192
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-9883
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9883
- https://bdu.fstec.ru/vul/2026-11116

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9879
BDU:2026-11113

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

98

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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9879
- https://security-tracker.debian.org/tracker/CVE-2026-9879
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/499129768
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9879
- https://security-tracker.debian.org/tracker/CVE-2026-9879
- https://bdu.fstec.ru/vul/2026-11113

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9891
BDU:2026-11118

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 9.0 AV:N/AC:H/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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9891
- https://security-tracker.debian.org/tracker/CVE-2026-9891
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513508128
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-9891
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9891
- https://bdu.fstec.ru/vul/2026-11118

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9893
BDU:2026-11119

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

100

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9893
- https://security-tracker.debian.org/tracker/CVE-2026-9893
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/513972075
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9893
- https://bdu.fstec.ru/vul/2026-11119

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9894
BDU:2026-11120

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9894
- https://security-tracker.debian.org/tracker/CVE-2026-9894
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/507707838
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9894
- https://bdu.fstec.ru/vul/2026-11120

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9896
BDU:2026-11121

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9896
- https://security-tracker.debian.org/tracker/CVE-2026-9896
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/508811474
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9896
- https://bdu.fstec.ru/vul/2026-11121

103

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-9887
BDU:2026-11117

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 148.0.7778.215
Microsoft Edge: до 148.0.3967.96
Debian GNU/Linux: 13
Astra Linux Special Edition: 1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.8 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: 2026-08-03 / 2026-08-03

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-9887
- https://security-tracker.debian.org/tracker/CVE-2026-9887
- https://chromereleases.googleblog.com/2026/05/stable-channel-update-for-desktop_0877304591.html
- https://issues.chromium.org/issues/511249104
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0723SE18HF
- https://security-tracker.debian.org/tracker/CVE-2026-9887
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-9887
- https://bdu.fstec.ru/vul/2026-11117

Краткое описание: Выполнение произвольного кода в Cisco SD-WAN

Идентификатор уязвимости: CVE-2026-20304
BDU:2026-11226

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Cisco SD-WAN: до 20.9 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K
- https://bdu.fstec.ru/vul/2026-11226

Краткое описание: Отказ в обслуживании в Cisco IOS XE

Идентификатор уязвимости: CVE-2026-20124
BDU:2026-11237

Идентификатор программной ошибки: CWE-772 Удержание ресурса после его использования

Уязвимый продукт: Cisco IOS XE: 17.18.1y

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

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.7 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: 2026-08-07 / 2026-08-07

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-snmp-dos-ZAqNm4MD
- https://bdu.fstec.ru/vul/2026-11237

106

Краткое описание: Отказ в обслуживании в Cisco IOS XE

Идентификатор уязвимости: CVE-2026-20301
BDU:2026-11236

Идентификатор программной ошибки: CWE-606 Отсутствует проверка входных данных для циклических операций

Уязвимый продукт: Cisco IOS XE: 26.2.1ea
Cisco IOS: 15.9(3)M14

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xmcp-thbAr34t
- https://bdu.fstec.ru/vul/2026-11236

Краткое описание: Выполнение произвольного кода в Cisco IOS XE

Идентификатор уязвимости: CVE-2026-20267
BDU:2026-11229

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Cisco IOS XE: 27.1.1

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

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.0 AV:N/AC:H/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: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxe-V8NMuMZJ
- https://bdu.fstec.ru/vul/2026-11229

Краткое описание: Выполнение произвольного кода в Cisco SD-WAN

Идентификатор уязвимости: CVE-2026-20303
BDU:2026-11228

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Cisco SD-WAN: до 20.9 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

1
0
8

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K
- https://bdu.fstec.ru/vul/2026-11228

109

Краткое описание: Выполнение произвольного кода в Cisco SD-WAN

Идентификатор уязвимости: CVE-2026-20310
BDU:2026-11227

Идентификатор программной ошибки: CWE-59 Некорректное разрешение ссылки перед доступом к файлу ("переход по ссылке")

Уязвимый продукт: Cisco SD-WAN: до 20.9 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K
- https://bdu.fstec.ru/vul/2026-11227

110

Краткое описание: Отказ в обслуживании в Cisco IOS XE

Идентификатор уязвимости: CVE-2026-20273
BDU:2026-11225

Идентификатор программной ошибки: CWE-74 Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение)

Уязвимый продукт: Cisco IOS XE: 27.1.1

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxe-V8NMuMZJ
- https://bdu.fstec.ru/vul/2026-11225

Краткое описание: Повышение привилегий в Integrated Management Controller

Идентификатор уязвимости: CVE-2026-20200
BDU:2026-11238

Идентификатор программной ошибки: CWE-141 Некорректная нейтрализация разделителей параметров или аргументов

Уязвимый продукт: Integrated Management Controller: до 6.0(2.260143)

Категория уязвимого продукта: Программно-аппаратное решение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-07 / 2026-08-07

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-arg-inject-upSHdMfU
- https://www.helpnetsecurity.com/2026/08/06/cisco-imc-cve-2026-20200-public-poc-exploit/
- https://github.com/NSIDE-ATTACK-LOGIC/CIMCown
- https://bdu.fstec.ru/vul/2026-11238

Краткое описание: Отказ в обслуживании в Cisco IOS XE

Идентификатор уязвимости: CVE-2026-20270
BDU:2026-11223

Идентификатор программной ошибки: CWE-682 Некорректные расчеты

Уязвимый продукт: Cisco IOS XE: 27.1.1

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxe-V8NMuMZJ
- https://bdu.fstec.ru/vul/2026-11223

Краткое описание: Отказ в обслуживании в Cisco IOS XE

Идентификатор уязвимости: CVE-2026-20269
BDU:2026-11222

Идентификатор программной ошибки: CWE-664 Некорректное обращение с ресурсом на протяжении его жизненного цикла

Уязвимый продукт: Cisco IOS XE: 27.1.1

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxe-V8NMuMZJ
- https://bdu.fstec.ru/vul/2026-11222

Краткое описание: Выполнение произвольного кода в Cisco IOS XE

Идентификатор уязвимости: CVE-2026-20272
BDU:2026-11221

Идентификатор программной ошибки: CWE-74 Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение)

Уязвимый продукт: Cisco IOS XE: 27.1.1

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

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

1 1 4

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxe-V8NMuMZJ
- https://bdu.fstec.ru/vul/2026-11221

Краткое описание: Отказ в обслуживании в Cisco IOS XE

Идентификатор уязвимости: CVE-2026-20268
BDU:2026-11220

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

Уязвимый продукт: Cisco IOS XE: 27.1.1

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxe-V8NMuMZJ
- https://bdu.fstec.ru/vul/2026-11220

116

Краткое описание: Выполнение произвольного кода в Electron

Идентификатор уязвимости: CVE-2026-70601
BDU:2026-11216

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Electron: до 42.0.0-beta.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://dailycve.com/electron-context-isolation-bypass-via-functionprototypebind-hijack-cve-2026-70601-dc-aug2026-1383/
- https://github.com/electron/electron/security/advisories/GHSA-h7rp-cf8h-j98x
- https://bdu.fstec.ru/vul/2026-11216

Краткое описание: Отказ в обслуживании в Cisco IOS XE

Идентификатор уязвимости: CVE-2026-20271
BDU:2026-11224

Идентификатор программной ошибки: CWE-691 Некорректное управление ходом выполнения команд

Уязвимый продукт: Cisco IOS XE: 27.1.1

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-06 / 2026-08-06

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-iosxe-V8NMuMZJ
- https://bdu.fstec.ru/vul/2026-11224

Краткое описание: Отказ в обслуживании в NGINX Ingress Controller

Идентификатор уязвимости: CVE-2026-55723
BDU:2026-11310

Идентификатор программной ошибки: CWE-76 Некорректная нейтрализация эквивалентов специальных элементов

Уязвимый продукт: NGINX Ingress Controller: от 3.6.0 до 3.7.2 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 8.3 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://my.f5.com/manage/s/article/K000161800
- https://bdu.fstec.ru/vul/2026-11310

Краткое описание: Выполнение произвольного кода в Splunk Enterprise

Идентификатор уязвимости: CVE-2026-20296
BDU:2026-11317

Идентификатор программной ошибки: CWE-352 Подделка межсайтового запроса (CSRF)

Уязвимый продукт: Splunk Enterprise: от 9.4.0 до 9.4.12 включительно
Splunk Cloud Platform: до 10.3.2512.16

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.3 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:L

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-16 / 2026-07-16

Ссылки на источник:

- https://advisory.splunk.com/advisories/SVD-2026-0702
- https://1275.ru/vulnerability/splunk-zakryl-tri-uyazvimosti-v-enterprise-i-cloud-platform-ot-podmeny-zaprosov-do-utechki-heshey-paroley_32225
- https://bdu.fstec.ru/vul/2026-11317

119

120

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31432
BDU:2026-11322

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: 7.0 rc6
Ubuntu: 24.04 LTS
Debian GNU/Linux: 13
Татлин-Обджект: до 1.12

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-08-07 / 2026-08-07

Ссылки на источник:

- https://git.kernel.org/stable/c/075ea208c648cc2bcd616295b711d3637c61de45
- https://git.kernel.org/stable/c/515c2daab46021221bdf406bef19bc90a44ec617
- https://git.kernel.org/stable/c/850452af77f55d185f9445e1f7a1db53c5e4aad4
- https://git.kernel.org/stable/c/d48c64fb80ad78b3dd29fb7d79b6ec7bd72bfc09
- https://git.kernel.org/stable/c/fda9522ed6afaec45cabc198d8492270c394c7bc
- https://security-tracker.debian.org/tracker/CVE-2026-31432
- https://ubuntu.com/security/CVE-2026-31432
- https://bdu.fstec.ru/vul/2026-11322

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43341
BDU:2026-11320

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

Уязвимый продукт: Linux: от 5.15 до 6.1.167 включительно
Татлин-Обджект: до 1.12

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-27 / 2026-07-27

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2026-43341
- https://git.kernel.org/stable/c/e96d48b37708d53cbdc47f6f60b0714fc4a5f596
- https://git.kernel.org/stable/c/d1b041080086e91d3733a5438a8c51ad5d3d8e09
- https://git.kernel.org/stable/c/77695a69baca9b99d95fad09fc78c2318736604f
- https://git.kernel.org/stable/c/184d2e9db27c0f76226b5cad16fe29510a5d2280
- https://git.kernel.org/stable/c/d6e1c9b02d85a4f1f4ba6d68e916d9b610a3ed7d
- https://git.kernel.org/linus/5e67ba9bb531e1ec6599a82a065dea9040b9ce50
- https://bdu.fstec.ru/vul/2026-11320

1
2
1

Краткое описание: Получение конфиденциальной информации в VMware vCenter Server

Идентификатор уязвимости: CVE-2026-59309
BDU:2026-11334

Идентификатор программной ошибки: CWE-303 Некорректная реализация алгоритма аутентификации

Уязвимый продукт: VMware vCenter Server: до 8.0 U3k
VMware Cloud Foundation: до 8.0 U3k
VMware Telco Cloud Platform: до KB449886
VMware Telco Cloud Infrastructure: до KB449886
VMware vSphere Foundation: до 9.0.2.0100

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017
- https://thehackernews.com/2026/07/three-critical-vmware-flaws-allow-auth.html
- https://github.com/vmware/vcf-security-and-compliance-guidelines/tree/main/security-advisories/vmsa-2026-0006
- https://bdu.fstec.ru/vul/2026-11334

Краткое описание: Выполнение произвольного кода в VMware vCenter Server

Идентификатор уязвимости: CVE-2026-59310
BDU:2026-11333

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

Уязвимый продукт: VMware vCenter Server: до 8.0 U3k
VMware Cloud Foundation: до 8.0 U3k
VMware Telco Cloud Platform: до KB449886
VMware Telco Cloud Infrastructure: до KB449886
VMware vSphere Foundation: до 9.0.2.0100

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

1
2
3

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017
- https://thehackernews.com/2026/07/three-critical-vmware-flaws-allow-auth.html
- https://github.com/vmware/vcf-security-and-compliance-guidelines/tree/main/security-advisories/vmsa-2026-0006
- https://github.com/HORKimhab/CVE-2026-59310
- https://bdu.fstec.ru/vul/2026-11333

Краткое описание: Выполнение произвольного кода в VMware ESXi

Идентификатор уязвимости: CVE-2026-47876
BDU:2026-11332

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: VMware ESXi: до ESXi80U3k-25595708
VMware Cloud Foundation: до ESXi-9.0.2.0100-25595025
VMware Telco Cloud Platform: до KB449886
VMware vSphere Foundation: до ESXi-9.0.2.0100-25595025

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.3 AV:L/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-30 / 2026-07-30

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017
- https://thehackernews.com/2026/07/three-critical-vmware-flaws-allow-auth.html
- https://github.com/vmware/vcf-security-and-compliance-guidelines/tree/main/security-advisories/vmsa-2026-0006
- https://bdu.fstec.ru/vul/2026-11332

1
2
4

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43084
BDU:2026-11331

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.19.4 до 6.19.14
Red Hat Enterprise Linux: 9
Ubuntu: 26.04 LTS
Татлин-Обджект: до 1.12

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://git.kernel.org/stable/c/22730cb96093b5be0609063bbb1923dbecd61252
- https://git.kernel.org/stable/c/41e3652a178cb0eecd48e0e6e27fbb73a004046a
- https://git.kernel.org/stable/c/9e5ebef91120d2764aefe557c3a484b6288f341f
- https://git.kernel.org/stable/c/936206e3f6ff411581e615e930263d6f8b78df9d
- https://access.redhat.com/security/cve/cve-2026-43084
- https://ubuntu.com/security/CVE-2026-43084
- https://bdu.fstec.ru/vul/2026-11331

126

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43334
BDU:2026-11330

Идентификатор программной ошибки: CWE-322 Обмен ключами без аутентификации субъекта

Уязвимый продукт: Linux: от 3.3 до 5.10.253
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Татлин-Обджект: до 1.12

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

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://git.kernel.org/stable/c/425a22c5373d4e1b46492ab869074ebeeade61f3
- https://git.kernel.org/stable/c/7ab69426e7ecbd18a222ee2ec87ca612d30197d7
- https://git.kernel.org/stable/c/01bb4045d2306c266178f49ce0c3576d237a3040
- https://git.kernel.org/stable/c/91649c02c1baaa18cedf7fb425fa1f0f852c8183
- https://git.kernel.org/stable/c/c8ff0ca6508535bccabd81c5c9dcc63de8a3d4fb
- https://git.kernel.org/stable/c/fa14e0e19820b1bbdb42185c9c4efa950bcffef9
- https://git.kernel.org/stable/c/ec17efb1ef91506cfd17a77692eaf4bbacb520ea

- https://git.kernel.org/stable/c/d05111bfe37bfd8bd4d2dfe6675d6bdeef43f7c7
- https://security-tracker.debian.org/tracker/CVE-2026-43334
- https://access.redhat.com/security/cve/cve-2026-43334
- https://ubuntu.com/security/CVE-2026-43334
- https://bdu.fstec.ru/vul/2026-11330

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-31444
BDU:2026-11319

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: 7.0 rc4
Ubuntu: 24.04 LTS
Татлин-Обджект: до 1.12

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-07 / 2026-08-07

Ссылки на источник:

- https://git.kernel.org/stable/c/48623ec358c1c600fa1e38368746f933e0f1a617
- https://git.kernel.org/stable/c/6d7e5a918c1d0aad06db0e17677b66fc9a471021
- https://git.kernel.org/stable/c/7de55bba69cbf0f9280daaea385daf08bc076121
- https://git.kernel.org/stable/c/9e785f004cbc56390479b77375726ea9b0d1a8a6

- https://git.kernel.org/stable/c/a5c6f6d6ceefed2d5210ee420fb75f8362461f46
- https://ubuntu.com/security/CVE-2026-31444
- https://bdu.fstec.ru/vul/2026-11319

128

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46129
BDU:2026-11329

Идентификатор программной ошибки: CWE-763 Освобождение недопустимого указателя или ссылки

Уязвимый продукт: Linux: 6.19
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Татлин-Обджект: до 1.12

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://git.kernel.org/stable/c/3f487be81292702a59ea9dbc4088b3360a50e837
- https://git.kernel.org/stable/c/9a060970fd7b5e1c561e4ce73cb9949e4269a738
- https://git.kernel.org/stable/c/ae6d6e31ceb72b7697c28a528e4923c08e3c2ef5
- https://git.kernel.org/stable/c/c2670ec4aa49ca226bce9776601e0da37502be07

- https://git.kernel.org/stable/c/dd6ade0fdd59218d71a981ae7c937a304e49209c
- https://git.kernel.org/stable/c/f414b3abbba59ef379a2b3c31f2bdd9358ed5e53
- https://security-tracker.debian.org/tracker/CVE-2026-46129
- https://ubuntu.com/security/CVE-2026-46129
- https://bdu.fstec.ru/vul/2026-11329

129

Краткое описание: Перезапись произвольных файлов в Linux

Идентификатор уязвимости: CVE-2026-46119
BDU:2026-11327

Идентификатор программной ошибки: CWE-131 Некорректный расчет размера буфера

Уязвимый продукт: Linux: от 6.7 до 6.12.88
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Татлин-Обджект: до 1.12

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Перезапись произвольных файлов

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://git.kernel.org/stable/c/1c439de70b1c3eb3c6bffa8245c16b9fc318f114
- https://git.kernel.org/stable/c/2ae0afd98432536562fa8261538ae795446f0589

- https://git.kernel.org/stable/c/38fdf04c602d52c42c67fc1617211492753b7e8b
- https://git.kernel.org/stable/c/408e85ee708b6aa03eeb0220ffa0915f4d407181
- https://git.kernel.org/stable/c/8517b6c8d2c759918ba0058cb6c7e14d59643202
- https://git.kernel.org/stable/c/b7df9fbd4869fdfe09a3f501ffd228486521e062
- https://git.kernel.org/stable/c/c2374b92c729d0388a538b3cde7b3e3b5e55ef39
- https://security-tracker.debian.org/tracker/CVE-2026-46119
- https://access.redhat.com/security/cve/cve-2026-46119
- https://ubuntu.com/security/CVE-2026-46119
- https://bdu.fstec.ru/vul/2026-11327

Краткое описание: Перезапись произвольных файлов в Linux

Идентификатор уязвимости: CVE-2026-46155
BDU:2026-11326

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

Уязвимый продукт: Linux: 7.1 rc2
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Татлин-Обджект: до 1.12

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Перезапись произвольных файлов

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-08-10 / 2026-08-10

Ссылки на источник:

- https://git.kernel.org/stable/c/512d33bc8ea4ea5c19728ee118715f4b1f4d1926
- https://git.kernel.org/stable/c/8d09328dfda089675e4c049f3f256064a1d1996b
- https://git.kernel.org/stable/c/9b3af35645ff9cd334edc130249f9a2fb2bea25f
- https://git.kernel.org/stable/c/a16f70a71be4b5a4eccf39a9bf09b47285f4cb7c
- https://git.kernel.org/stable/c/dffb44b2e06a2908e249f0f93156fc987eee1d1c
- https://security-tracker.debian.org/tracker/CVE-2026-46155
- https://access.redhat.com/security/cve/cve-2026-46155
- https://ubuntu.com/security/CVE-2026-46155
- https://bdu.fstec.ru/vul/2026-11326