НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-07-23.1 | 23 июля 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2026-49049	Joomla	Сетевой	OAF	2026-06-29	✓
2	Высокая	CVE-2026-31431	Linux	Локальный	PE	2026-04-30	✓
3	Критическая	CVE-2026-46901	Oracle Enterprise Command Center Framework	Сетевой	DoS	2026-06-18	✓
4	Высокая	CVE-2026-0271	Prisma Access Agent	Локальный	PE	2026-06-16	✓
5	Высокая	CVE-2026-44883	Portainer	Сетевой	OSI	2026-06-10	✓
6	Высокая	CVE-2026-45469	Microsoft Excel	Локальный	ACE	2026-06-16	✓
7	Высокая	CVE-2026-40409	Windows Universal Disk	Локальный	PE	2026-06-16	✓
8	Высокая	CVE-2026-50107	NGINX Gateway Fabric	Сетевой	DoS	2026-06-23	✓
9	Высокая	CVE-2026-11698	Google Chrome	Сетевой	ACE	2026-06-10	✓
10	Высокая	CVE-2026-11694	Google Chrome	Сетевой	ACE	2026-06-10	✓
11	Высокая	CVE-2026-11699	Google Chrome	Сетевой	ACE	2026-06-10	✓
12	Высокая	CVE-2026-11690	Google Chrome	Сетевой	ACE	2026-06-10	✓
13	Высокая	CVE-2026-11688	Google Chrome	Сетевой	ACE	2026-06-10	✓

14	Высокая	CVE-2026-11687	Google Chrome	Сетевой	ACE	2026-06-10	✓
15	Высокая	CVE-2026-46522	ImageMagick	Сетевой	DoS	2026-06-10	✓
16	Высокая	CVE-2026-45486	Microsoft Office	Локальный	ACE	2026-06-16	✓
17	Критическая	CVE-2026-46773	Oracle Unified Directory	Сетевой	ACE	2026-06-23	✓
18	Критическая	CVE-2026-46860	MySQL Router	Сетевой	ACE	2026-06-18	✓
19	Критическая	CVE-2026-46880	JD Edwards EnterpriseOne Tools	Сетевой	ACE	2026-06-24	✓
20	Критическая	CVE-2026-55200	libssh2	Сетевой	ACE	2026-06-24	✓
21	Критическая	CVE-2026-46792	Identity Manager Connector	Сетевой	ACE	2026-06-23	✓
22	Критическая	CVE-2026-46807	Oracle Identity Manager	Сетевой	ACE	2026-06-24	✓
23	Критическая	CVE-2026-33757	OpenBao	Сетевой	OSI	2026-06-19	✓
24	Высокая	CVE-2026-43055	Linux	Сетевой	DoS	2026-05-05	✓
25	Критическая	CVE-2026-34286	Identity Manager Connector	Сетевой	DoS	2026-04-24	✓
26	Высокая	CVE-2026-43049	Linux	Локальный	DoS	2026-05-05	✓
27	Высокая	CVE-2026-43051	Linux	Смежная сеть	DoS	2026-05-05	✓
28	Высокая	CVE-2026-43047	Linux	Локальный	DoS	2026-05-05	✓

29	Критическая	CVE-2026-46803	Oracle WebCenter Portal	Сетевой	ACE	2026-06-24	✓
30	Критическая	CVE-2026-46774	Oracle Unified Directory	Сетевой	ACE	2026-06-24	✓
31	Высокая	CVE-2026-45156	Nextcloud	Сетевой	PE	2026-06-25	✓
32	Высокая	CVE-2026-34305	WebLogic Server	Сетевой	OSI	2026-04-23	✓
33	Критическая	CVE-2026-43038	Linux	Сетевой	DoS	2026-05-05	✓
34	Критическая	CVE-2026-48773	ProxySQL	Сетевой	ACE	2026-06-24	✓
35	Высокая	CVE-2026-31696	Linux	Локальный	DoS	2026-05-05	✓
36	Высокая	CVE-2026-31680	Linux	Локальный	DoS	2026-04-29	✓
37	Высокая	CVE-2026-31683	Linux	Локальный	DoS	2026-04-29	✓
38	Критическая	CVE-2026-52813	Gogs	Сетевой	ACE	2026-06-26	✓
39	Критическая	CVE-2026-31685	Linux	Сетевой	DoS	2026-04-29	✓
40	Высокая	CVE-2025-71089	Linux	Локальный	DoS	2026-02-04	✓
41	Высокая	CVE-2025-71159	Linux	Локальный	DoS	2026-02-04	✓
42	Высокая	CVE-2026-32208	Microsoft Edge	Сетевой	LoI	2026-06-26	✓
43	Критическая	CVE-2026-48582	Microsoft Exchange Online	Сетевой	PE	2026-06-26	✓

44	Критическая	CVE-2026-47647	Microsoft Dynamics 365	Сетевой	PE	2026-06-26	✓
45	Высокая	CVE-2026-43503	Linux	Локальный	PE	2026-06-29	✓
46	Высокая	CVE-2026-34291	Oracle HTTP Server	Сетевой	ACE	2026-04-27	✓
47	Высокая	CVE-2026-22010	Financial Services Analytical Applications Infrastructure	Сетевой	ACE	2026-04-27	✓
48	Высокая	CVE-2026-35243	Application Development Framework	Локальный	ACE	2026-04-27	✓
49	Высокая	CVE-2026-1519	Red Hat Enterprise Linux	Сетевой	DoS	2026-06-29	✓
50	Высокая	CVE-2026-47645	Microsoft 365 Copilot	Сетевой	PE	2026-06-26	✓
51	Высокая	CVE-2026-35231	Financial Services Transaction Filtering	Сетевой	ACE	2026-04-24	✓
52	Высокая	CVE-2026-34320	Oracle Financial Services Customer Screening	Сетевой	ACE	2026-04-27	✓
53	Высокая	CVE-2026-43499	Linux	Локальный	ACE	2026-02-09	✓
54	Высокая	CVE-2026-46748	SINEC INS	Сетевой	PE	2026-06-23	✓
55	Критическая	CVE-2026-49268	Apache Shiro	Сетевой	SB	2026-06-30	✓
56	Критическая	CVE-2026-49871	Apache APISIX	Сетевой	LoI	2026-06-30	✓
57	Критическая	CVE-2026-45480	Azure Active Directory (AAD)	Сетевой	PE	2026-06-26	✓
58	Высокая	CVE-2026-20103	Cisco	Сетевой	DoS	2026-06-17	✓

59	Критическая	CVE-2026-39999	Apache APISIX	Сетевой	SB	2026-06-30	✓
60	Высокая	CVE-2026-39998	Apache APISIX	Сетевой	SB	2026-06-30	✓
61	Критическая	CVE-2026-56141	JetBrains Hub	Сетевой	ACE	2026-06-30	✓
62	Критическая	CVE-2026-58053	Gitea	Сетевой	PE	2026-06-30	✓
63	Высокая	CVE-2026-44728	babel	Локальный	ACE	2026-06-01	✓
64	Высокая	CVE-2025-12659	Simcenter Femap	Локальный	ACE	2026-05-20	✓
65	Высокая	CVE-2026-33893	Siemens Teamcenter	Сетевой	OSI	2026-05-20	✓
66	Высокая	CVE-2026-27877	Grafana	Сетевой	OSI	2026-06-09	✓
67	Высокая	CVE-2024-34459	Libxml2	Сетевой	PE	2026-07-01	✓
68	Критическая	CVE-2026-46817	E-Business Suite	Сетевой	ACE	2026-06-30	✓
69	Высокая	CVE-2026-10712	Gitlab	Сетевой	ACE	2026-07-01	✓
70	Высокая	CVE-2026-12053	Gitlab	Сетевой	OSI	2026-07-01	✓
71	Высокая	CVE-2026-10911	Google Chrome	Сетевой	SB	2026-07-02	✓
72	Критическая	CVE-2026-48281	ColdFusion	Сетевой	ACE	2026-04-15	✓
73	Критическая	CVE-2026-48277	ColdFusion	Сетевой	ACE	2026-04-15	✓

74	Высокая	CVE-2026-11024	Google Chrome	Сетевой	DoS	2026-07-01	✓
75	Критическая	CVE-2026-48316	ColdFusion	Сетевой	ACE	2026-04-15	✓
76	Высокая	CVE-2026-10907	Google Chrome	Сетевой	ACE	2026-07-02	✓
77	Высокая	CVE-2026-10937	Google Chrome	Сетевой	SB	2026-07-02	✓
78	Высокая	CVE-2026-10947	Google Chrome	Сетевой	ACE	2026-07-02	✓
79	Высокая	CVE-2026-10929	Google Chrome	Сетевой	SB	2026-07-02	✓
80	Высокая	CVE-2026-10938	Google Chrome	Сетевой	SB	2026-07-02	✓
81	Высокая	CVE-2026-10882	Google Chrome	Сетевой	ACE	2026-07-02	✓
82	Высокая	CVE-2026-11019	Google Chrome	Сетевой	SB	2026-07-01	✓
83	Высокая	CVE-2026-11010	Google Chrome	Сетевой	SB	2026-07-01	✓
84	Высокая	CVE-2026-44577	Next.js	Сетевой	DoS	2026-06-29	✓
85	Высокая	CVE-2026-44579	Next.js	Сетевой	DoS	2026-06-29	✓
86	Высокая	CVE-2026-44575	Next.js	Сетевой	OSI	2026-06-29	✓
87	Высокая	CVE-2026-11040	Google Chrome	Сетевой	SB	2026-07-01	✓
88	Высокая	CVE-2026-44290	protobufjs	Сетевой	DoS	2026-06-29	✓

89	Высокая	CVE-2026-45033	GitHub Copilot	Локальный	ACE	2026-06-30	✓
90	Высокая	VE-2026-11000	Google Chrome	Сетевой	ACE	2026-07-01	✓
91	Критическая	CVE-2026-11002	Google Chrome	Сетевой	SB	2026-07-01	✓
92	Высокая	CVE-2026-44293	protobufjs	Сетевой	ACE	2026-06-29	✓
93	Высокая	CVE-2025-26842	Znuny	Сетевой	OSI	2025-03-06	✓
94	Высокая	CVE-2026-11041	Google Chrome	Сетевой	SB	2026-07-01	✓
95	Высокая	CVE-2026-44289	protobufjs	Сетевой	DoS	2026-06-29	✓
96	Высокая	CVE-2026-7815	pgAdmin 4	Сетевой	ACE	2026-07-01	✓
97	Высокая	CVE-2026-10887	Google Chrome	Сетевой	ACE	2026-07-02	✓
98	Критическая	CVE-2026-11047	Google Chrome	Сетевой	SB	2026-07-01	✓
99	Высокая	CVE-2026-7819	pgAdmin 4	Сетевой	OAF	2026-07-01	✓
100	Высокая	CVE-2026-7818	pgAdmin 4	Локальный	ACE	2026-07-01	✓
101	Высокая	CVE-2026-7816	pgAdmin 4	Сетевой	ACE	2026-07-01	✓
102	Высокая	CVE-2026-32658	Dell Automation Platform	Сетевой	PE	2026-06-23	✓
103	Высокая	CVE-2026-10885	Google Chrome	Сетевой	ACE	2026-07-02	✓

104	Высокая	CVE-2026-10891	Google Chrome	Сетевой	ACE	2026-07-02	✓
105	Высокая	CVE-2026-47633	Microsoft Cost Management	Сетевой	OSI	2026-06-26	✓
106	Высокая	CVE-2026-20215	Secure Endpoint Private Cloud	Сетевой	DoS	2026-07-03	✓
107	Высокая	CVE-2026-20244	Secure Endpoint Private Cloud	Сетевой	DoS	2026-07-03	✓
108	Высокая	CVE-2026-20243	Secure Endpoint Private Cloud	Сетевой	DoS	2026-07-03	✓
109	Высокая	CVE-2026-20217	Secure Endpoint Private Cloud	Сетевой	DoS	2026-07-03	✓
110	Высокая	CVE-2026-20214	Secure Endpoint Private Cloud	Сетевой	DoS	2026-07-03	✓
111	Высокая	CVE-2025-39793	Linux	Локальный	ACE	2026-02-11	✓
112	Высокая	CVE-2026-0241	Trust Protection Foundation	Сетевой	ACE	2026-05-21	✓
113	Высокая	CVE-2026-41702	VMware Fusion	Локальный	PE	2026-05-20	✓
114	Высокая	CVE-2026-20213	Secure Endpoint Private Cloud	Сетевой	DoS	2026-07-03	✓
115	Критическая	CVE-2026-48307	ColdFusion	Сетевой	ACE	2025-12-10	✓
116	Высокая	CVE-2026-48285	ColdFusion	Сетевой	RLF	2025-07-11	✓
117	Высокая	CVE-2026-44432	Python	Сетевой	DoS	2026-06-29	✓
118	Критическая	CVE-2026-4858	Mattermost	Сетевой	OSI	2025-02-26	✓

119	Критическая	CVE-2026-12046	pgAdmin 4	Сетевой	ACE	2026-07-06	✓
120	Высокая	CVE-2026-42504	Go	Сетевой	DoS	2026-07-03	✓
121	Высокая	CVE-2026-27145	Go	Сетевой	DoS	2026-07-03	✓
122	Критическая	CVE-2026-46896	Oracle Enterprise Command Center Framework	Сетевой	ACE	2026-07-06	✓
123	Критическая	CVE-2026-8452	NetScaler Gateway	Сетевой	DoS	2026-07-06	✓
124	Высокая	CVE-2026-10816	NetScaler Gateway	Сетевой	OSI	2026-07-06	✓
125	Высокая	CVE-2026-58465	Eclipse Wakaama	Сетевой	DoS	2026-07-06	✓
126	Критическая	CVE-2026-43898	SandboxJS	Сетевой	ACE	2026-06-29	✓
127	Критическая	CVE-2026-12045	pgAdmin 4	Сетевой	ACE	2026-07-06	✓
128	Высокая	CVE-2026-41053	Rancher	Сетевой	OSI	2026-07-06	✓
129	Высокая	CVE-2026-46242	Linux	Локальный	ACE	2026-07-06	✓
130	Критическая	CVE-2026-22874	Gitea	Сетевой	RLF	2026-07-06	✓
131	Критическая	CVE-2026-48283	ColdFusion	Сетевой	ACE	2025-12-10	✓
132	Высокая	CVE-2025-7737	Hitachi Virtual Storage Platform G1000	Сетевой	DoS	2026-07-06	✓
133	Высокая	CVE-2026-46915	E-Business Suite	Сетевой	ACE	2026-07-06	✓

134	Высокая	CVE-2026-46927	E-Business Suite	Сетевой	ACE	2026-07-06	✓
135	Критическая	CVE-2026-20181	Cisco Identity Services Engine	Сетевой	DoS	2026-07-06	✓

1

Краткое описание: Перезапись произвольных файлов в Joomla

Идентификатор уязвимости: CVE-2026-49049

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Helix3 с 1.0 по 3.1.1 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Перезапись произвольных файлов

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-29 / 2026-06-30

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-49049

2

Краткое описание: Повышение привилегий в Linux

Идентификатор уязвимости: CVE-2026-31431
BDU:2026-06123

Идентификатор программной ошибки: CWE-669 Некорректная передача ресурса между окружениями

Уязвимый продукт: Linux: от 6.7 до 6.12.85
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS
Suse Linux Enterprise Desktop: 15 SP7
Astra Linux Common Edition: 1.6 «Смоленск»
Debian GNU/Linux: 13
SUSE Linux Enterprise High Performance Computing: 15 SP7
РЕД ОС: 8.0
SUSE Linux Enterprise High Availability Extension: 15 SP7
ОСОН ОСнова Onyx: 2.15
Astra Linux Special Edition: 4.8
SUSE Linux Enterprise Micro: 5.5
Альт 8 СП: -
Циркон 37К: z37k-2057
АЛЬТ СП 10: -
Platform V SberLinux OS Server: до 9.2.3-fstec
Горизонт-ВС: 40-17-37-17

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-30 / 2026-06-17

Ссылки на источник:

- http://www.openwall.com/lists/oss-security/2026/04/29/26
- https://access.redhat.com/security/cve/cve-2026-31431
- https://altsp.su/obnovleniya-bezopasnosti/
- https://git.kernel.org/linus/a664bf3d603dc3bdcf9ae47cc21e0daec706d7a5
- https://git.kernel.org/stable/c/a664bf3d603dc3bdcf9ae47cc21e0daec706d7a5
- https://git.kernel.org/stable/c/ce42ee423e58dffa5ec03524054c9d8bfd4f6237
- https://git.kernel.org/stable/c/fafe0fa2995a0f7073c1c358d7d3145bcc9aedd8
- https://github.com/insomnisec/Detections-CVE-2026-31431
- https://github.com/rootsecdev/cve_2026_31431
- https://github.com/theori-io/copy-fail-CVE-2026-31431
- https://lore.kernel.org/linux-cve-announce/2026042214-CVE-2026-31431-3d65@gregkh/
- https://nvd.nist.gov/vuln/detail/CVE-2026-31431
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-kernel-lt-cve-2026-31431/
- https://security-tracker.debian.org/tracker/CVE-2026-31431
- https://ubuntu.com/security/CVE-2026-31431
- https://vuldb.com/vuln/358784
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-0512SE18MD
- https://wiki.astralinux.ru/x/3U8TH
- https://wiki.astralinux.ru/x/61ETH
- https://wiki.astralinux.ru/x/J1ITH
- https://wiki.astralinux.ru/x/KVITH
- https://wiki.astralinux.ru/x/PVITH
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://www.suse.com/security/cve/CVE-2026-31431.html
- https://поддержка.нппкт.рф/bin/view/ОСнова/Обновления/Оперативные_исправления/2026-04-30
- https://xint.io/blog/copy-fail-linux-distributions#the-fix-6
- https://wiki.astralinux.ru/astra-linux-se47-bulletin-2026-0518SE47
- https://altsp.su/obnovleniya-bezopasnosti/
- https://wiki.astralinux.ru/astra-linux-se17-bulletin-2026-0522SE17HF
- https://bdu.fstec.ru/vul/2026-06123

- https://bdu.fstec.ru/vul/2026-06123

3

Краткое описание: Отказ в обслуживании в Oracle Enterprise Command Center Framework

Идентификатор уязвимости: CVE-2026-46901
BDU:2026-08600

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Oracle Enterprise Command Center Framework: 16

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-18 / 2026-06-18

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-08600

4

Краткое описание: Повышение привилегий в Prisma Access Agent

Идентификатор уязвимости: CVE-2026-0271
BDU:2026-08603

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

Уязвимый продукт: Prisma Access Agent: до 26.2.1

Категория уязвимого продукта: Прикладное программное обеспечение

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:L/AC:L/PR:L/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: 2026-06-16 / 2026-06-16

Ссылки на источник:

- https://security.paloaltonetworks.com/CVE-2026-0271
- https://bdu.fstec.ru/vul/2026-08603

Краткое описание: Получение конфиденциальной информации в Portainer

Идентификатор уязвимости: CVE-2026-44883
BDU:2026-08588

Идентификатор программной ошибки: CWE-598 Разглашение информации через GET-запросы

Уязвимый продукт: РЕД ОС: 8.0
Portainer: от 2.40.0 до 2.41.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации.

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.

5

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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://github.com/advisories/GHSA-jvp4-q659-95mj
- https://github.com/portainer/portainer/security/advisories/GHSA-jvp4-q659-95mj
- https://github.com/portainer/portainer/releases/tag/2.33.8
- https://github.com/portainer/portainer/releases/tag/2.41.0
- https://github.com/portainer/portainer/releases/tag/2.39.2
- https://github.com/portainer/portainer
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-44883
- https://bdu.fstec.ru/vul/2026-08588

6

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-45469
BDU:2026-08585

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

Уязвимый продукт: Office Online Server: до 16.0.10417.20137
Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: до 16.110.26061317
Microsoft Excel 2016: до 16.0.5556.1001
Microsoft Office LTSC 2024: до 16.110.26061317
Microsoft Office 2019: -
Microsoft Office 365: до 16.110.26061317

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-16 / 2026-06-16

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45469
- https://bdu.fstec.ru/vul/2026-08585

7

Краткое описание: Повышение привилегий в Windows Universal Disk

Идентификатор уязвимости: CVE-2026-40409
BDU:2026-08586

Идентификатор программной ошибки: CWE-197 Ошибка числовых усечений

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9234
Windows 10 1809: до 10.0.17763.8880
Windows 10 21H2: до 10.0.19044.7417
Windows 10 22H2: до 10.0.19045.7417
Windows 11 23H2: до 10.0.22631.7219
Windows 11 24H2: до 10.0.26100.8655
Windows Server 2012: до 6.2.9200.26132
Windows Server 2012 R2: до 6.3.9600.23228
Windows Server 2012 (Server Core installation): до 6.2.9200.26132
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23228
Windows Server 2016: до 10.0.14393.9234
Windows Server 2016 (Server Core installation): до 10.0.14393.9234
Windows Server 2019: до 10.0.17763.8880
Windows Server 2019 (Server Core installation): до 10.0.17763.8880
Windows Server 2022: до 10.0.20348.5256
Windows Server 2022 (Server Core installation): до 10.0.20348.5256
Windows Server 2025: до 10.0.26100.32995
Windows Server 2025 (Server Core installation): до 10.0.26100.32995
Windows 11 25H2: до 10.0.26200.8655
Windows 11 26H1: до 10.0.28000.2269

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-16 / 2026-06-16

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40409
- https://bdu.fstec.ru/vul/2026-08586

8

Краткое описание: Отказ в обслуживании в NGINX Gateway Fabric

Идентификатор уязвимости: CVE-2026-50107
BDU:2026-08558

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

Уязвимый продукт: NGINX Gateway Fabric: от 2.3.0 до 2.6.3 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: 8.1 AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-23 / 2026-06-23

Ссылки на источник:

- https://my.f5.com/manage/s/article/K000161785
- https://bdu.fstec.ru/vul/2026-08558

9

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-11698
BDU:2026-08564

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.103

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
- https://issues.chromium.org/issues/518235412
- https://bdu.fstec.ru/vul/2026-08564

10

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-11694
BDU:2026-08571

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.103

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
- https://issues.chromium.org/issues/517705966
- https://bdu.fstec.ru/vul/2026-08571

11

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-11699
BDU:2026-08562

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.103

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
- https://issues.chromium.org/issues/518237527
- https://bdu.fstec.ru/vul/2026-08562

12

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-11690
BDU:2026-08575

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 149.0.7827.103

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
- https://issues.chromium.org/issues/517533654
- https://bdu.fstec.ru/vul/2026-08575

13

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-11688
BDU:2026-08577

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

Уязвимый продукт: Google Chrome: до 149.0.7827.103

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
- https://issues.chromium.org/issues/517309206
- https://bdu.fstec.ru/vul/2026-08577

14

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-11687
BDU:2026-08578

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.103

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop_0153744567.html
- https://issues.chromium.org/issues/517303276
- https://bdu.fstec.ru/vul/2026-08578

Краткое описание: Отказ в обслуживании в ImageMagick

Идентификатор уязвимости: CVE-2026-46522
BDU:2026-08580

Идентификатор программной ошибки: CWE-835 Бесконечный цикл (зацикливание)

Уязвимый продукт: ImageMagick: до 6.9.13-48
Debian GNU/Linux: 13
РЕД ОС: 8.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

15 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-06-10 / 2026-06-10

Ссылки на источник:

- https://github.com/advisories/GHSA-7gg8-qqx7-92g5
- https://github.com/ImageMagick/ImageMagick
- https://github.com/ImageMagick/ImageMagick/security/advisories/GHSA-7gg8-qqx7-92g5
- https://bdu.fstec.ru/vul/2026-08580

16

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-45486
BDU:2026-08584

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: до 16.110.26061317
Microsoft Office LTSC 2024: до 16.110.26061317
Microsoft Office 365: до 16.110.26061317

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-16 / 2026-06-16

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45486
- https://bdu.fstec.ru/vul/2026-08584

17

Краткое описание: Выполнение произвольного кода в Oracle Unified Directory

Идентификатор уязвимости: CVE-2026-46773
BDU:2026-08659

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Oracle Unified Directory: 14.1.2.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 9.8 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: 2026-06-23 / 2026-06-23

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-08659

18

Краткое описание: Выполнение произвольного кода в MySQL Router

Идентификатор уязвимости: CVE-2026-46860
BDU:2026-08662

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: MySQL Router: от 9.0.0 до 9.7.0 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 9.8 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: 2026-06-18 / 2026-06-18

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-08662

19

Краткое описание: Выполнение произвольного кода в JD Edwards EnterpriseOne Tools

Идентификатор уязвимости: CVE-2026-46880
BDU:2026-08638

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: JD Edwards EnterpriseOne Tools: от 9.2.0.0 до 9.2.26.2 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 9.8 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: 2026-06-24 / 2026-06-24

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-08638

20

Краткое описание: Выполнение произвольного кода в libssh2

Идентификатор уязвимости: CVE-2026-55200
BDU:2026-08612

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

Уязвимый продукт: libssh2: до 1.11.1 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 2026-06-24 / 2026-06-24

Ссылки на источник:

- https://github.com/libssh2/libssh2/commit/97acf3dfda80c91c3a8c9f2372546301d4a1a7a8
- https://github.com/bikini/exploitarium/tree/main/libssh2-cve-2026-55200-poc
- https://www.vulncheck.com/advisories/libssh2-out-of-bounds-write-via-unchecked-packet-length-in-transport-c
- https://vulners.com/cve/CVE-2026-55200
- https://web.archive.org/web/20260623211210/https://github.com/bikini/exploitarium/tree/main/libssh2-cve-2026-55200-poc
- https://bdu.fstec.ru/vul/2026-08612

21

Краткое описание: Выполнение произвольного кода в Identity Manager Connector

Идентификатор уязвимости: CVE-2026-46792
BDU:2026-08625

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Identity Manager Connector: 14.1.2.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 9.9 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: 2026-06-23 / 2026-06-23

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-08625

22

Краткое описание: Выполнение произвольного кода в Oracle Identity Manager

Идентификатор уязвимости: CVE-2026-46807
BDU:2026-08631

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

Уязвимый продукт: Identity Manager: 14.1.2.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2026-06-24 / 2026-06-24

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-08631

23

Краткое описание: Получение конфиденциальной информации в OpenBao

Идентификатор уязвимости: CVE-2026-33757
BDU:2026-08727

Идентификатор программной ошибки: CWE-384 Фиксация сессии

Уязвимый продукт: РЕД ОС: 8.0
OpenBao: до 2.5.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-19 / 2026-06-19

Ссылки на источник:

- https://github.com/advisories/GHSA-7q7g-x6vg-xpc3
- https://github.com/openbao/openbao/commit/e32103951925723e9787e33886ab6b6ec20f4964
- https://github.com/openbao/openbao
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-33757
- https://bdu.fstec.ru/vul/2026-08727

24

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43055
BDU:2026-08744

Идентификатор программной ошибки: CWE-456 Отсутствует инициализация переменной

Уязвимый продукт: Linux: от 6.16 до 6.18.22
Red Hat Enterprise Linux: 10

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026050108-CVE-2026-43055-5bb1@gregkh/
- https://git.kernel.org/stable/c/01f784fc9d0ab2a6dac45ee443620e517cb2a19b
- https://git.kernel.org/stable/c/4eaff1728d0e69b95933412241bbccf4f797dba8
- https://git.kernel.org/stable/c/ce54802fe6bb78eb0feffc66fed6a45d41ffc3ab
- https://access.redhat.com/security/cve/cve-2026-43055
- https://bdu.fstec.ru/vul/2026-08744

25

Краткое описание: Отказ в обслуживании в Identity Manager Connector

Идентификатор уязвимости: CVE-2026-34286
BDU:2026-08715

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

Уязвимый продукт: Identity Manager Connector: 12.2.1.4.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-24 / 2026-04-24

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpuapr2026.html
- https://bdu.fstec.ru/vul/2026-08715

26

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43049
BDU:2026-08747

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: до 6.12.81
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026050106-CVE-2026-43049-224e@gregkh/
- https://git.kernel.org/stable/c/772f99cc8d6e5d95613bce93c9624e154c1abe88
- https://git.kernel.org/stable/c/9a793ac19eb84f44ed759c0fce80cf29bc2a2453
- https://git.kernel.org/stable/c/b846fb0a73e99174f08238e083e284c0463a2102
- https://git.kernel.org/stable/c/f7a4c78bfeb320299c1b641500fe7761eadbd101
- https://security-tracker.debian.org/tracker/CVE-2026-43049
- https://access.redhat.com/security/cve/cve-2026-43049
- https://bdu.fstec.ru/vul/2026-08747

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43051
BDU:2026-08750

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: до 5.10.253
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13

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.

27

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026050107-CVE-2026-43051-0d15@gregkh/
- https://git.kernel.org/stable/c/2f1763f62909ccb6386ac50350fa0abbf5bb16a9
- https://git.kernel.org/stable/c/3d78386b144453c47e81bf62dc3601b757f02d99
- https://git.kernel.org/stable/c/41026bcc0fdf82605205c27935ef719cbc07193b
- https://git.kernel.org/stable/c/5b5b9730111808410e404ceac2fabd32eef92fbd
- https://git.kernel.org/stable/c/8bd690ac1242332c73cba10dacdad6c6642bbb94
- https://git.kernel.org/stable/c/c8dc23c97680eebefde06da5858aaef1b37cf75d
- https://git.kernel.org/stable/c/d0ae84b3c9f3ea1a564eb1b7612113ca9fe8aada
- https://git.kernel.org/stable/c/fa8901cb1f0b2113a342db93bd5684b59fe99dcf

- https://access.redhat.com/security/cve/cve-2026-43051
- https://security-tracker.debian.org/tracker/CVE-2026-43051
- https://bdu.fstec.ru/vul/2026-08750

28

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43047
BDU:2026-08738

Идентификатор программной ошибки: CWE-1012 Сквозные уязвимости

Уязвимый продукт: Linux: до 5.10.253
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026050105-CVE-2026-43047-13ab@gregkh/
- https://git.kernel.org/stable/c/2edc92f89eee328b5be5706b5d431bf90669e9c0
- https://git.kernel.org/stable/c/516da3f25cfe18643835af1cf09b0e9ffc36c383
- https://git.kernel.org/stable/c/6a4acd3e86fe5584050c213d95147eba33856033
- https://git.kernel.org/stable/c/74c6015375d8b9bc1b1eb79f20636c8e894bcad7
- https://git.kernel.org/stable/c/7f66fdbc077faed3b52519228d21d81979e92249
- https://git.kernel.org/stable/c/a61163daf8a90b4a7ef154d5fc9c525f665734e3
- https://git.kernel.org/stable/c/c7a27bb4d0f6573ca0f9c7ef0b63291486239190
- https://git.kernel.org/stable/c/e716edafedad4952fe3a4a273d2e039a84e8681a

- https://security-tracker.debian.org/tracker/CVE-2026-43047
- https://access.redhat.com/security/cve/cve-2026-43047
- https://bdu.fstec.ru/vul/2026-08738

29

Краткое описание: Выполнение произвольного кода в Oracle WebCenter Portal

Идентификатор уязвимости: CVE-2026-46803
BDU:2026-08710

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

Уязвимый продукт: Oracle WebCenter Portal: 14.1.2.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-24 / 2026-06-24

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-08710

30

Краткое описание: Выполнение произвольного кода в Oracle Unified Directory

Идентификатор уязвимости: CVE-2026-46774
BDU:2026-08708

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Oracle Unified Directory: 14.1.2.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 9.8 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: 2026-06-24 / 2026-06-24

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-08708

31

Краткое описание: Повышение привилегий в Nextcloud

Идентификатор уязвимости: CVE-2026-45156
BDU:2026-08694

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Nextcloud: до 8.3.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-25 / 2026-06-25

Ссылки на источник:

- https://github.com/cybertechajju/CVE-2026-45156-POC
- https://github.com/nextcloud/security-advisories/security/advisories/GHSA-qqgv-fqwp-mjpp
- https://hackerone.com/reports/3489490
- https://bdu.fstec.ru/vul/2026-08694

32

Краткое описание: Получение конфиденциальной информации в WebLogic Server

Идентификатор уязвимости: CVE-2026-34305
BDU:2026-08689

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

Уязвимый продукт: WebLogic Server: 15.1.1.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-23 / 2026-04-23

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpuapr2026.html
- https://bdu.fstec.ru/vul/2026-08689

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-43038
BDU:2026-08754

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

Уязвимый продукт: Linux: от 3.13 до 5.10.253
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Debian GNU/Linux: 13

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.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://git.kernel.org/stable/c/0452b6526b2f54b2413b9cb4ff1ea2ac542c99c7
- https://git.kernel.org/stable/c/1ceeebd5bd6d855b17a5df625109bfe29129d7cf
- https://git.kernel.org/stable/c/3d5127d998de617b130aae96b138dba22ac6a8a7
- https://git.kernel.org/stable/c/86ab3e55673a7a49a841838776f1ab18d23a67b5
- https://git.kernel.org/stable/c/a2edbb6393972a02114b6003953a5cef3104fada
- https://git.kernel.org/stable/c/a4437faf135da293d16fcc4cc607316742bd0ebb
- https://git.kernel.org/stable/c/c438ba010171b70bad22fc18b1d5bdc3627476e8
- https://git.kernel.org/stable/c/e41953e7d118e2702bcb217879c173d9d1d3cd4e
- https://lore.kernel.org/linux-cve-announce/2026050103-CVE-2026-43038-b591@gregkh/

- https://security-tracker.debian.org/tracker/CVE-2026-43038
- https://access.redhat.com/security/cve/cve-2026-43038
- https://bdu.fstec.ru/vul/2026-08754

34

Краткое описание: Выполнение произвольного кода в ProxySQL

Идентификатор уязвимости: CVE-2026-48773
BDU:2026-08692

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: ProxySQL: от 2.0.18 до 3.0.9

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2026-06-24 / 2026-06-24

Ссылки на источник:

- https://github.com/sysown/proxysql/releases/tag/v3.0.9
- https://bdu.fstec.ru/vul/2026-08692

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31696
BDU:2026-08757

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: до 7.1 rc1
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13

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.

35

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026050118-CVE-2026-31696-d2de@gregkh/
- https://git.kernel.org/stable/c/1fa36cf495b0023e8475d038535c05e4063211e1
- https://git.kernel.org/stable/c/4458757c020592a3094366e0fb20457383b42f92
- https://git.kernel.org/stable/c/a1be1c9ece26cea69654f28b255ff9a7906b897b
- https://git.kernel.org/stable/c/ac33733b10b484d666f97688561670afd5861383
- https://git.kernel.org/stable/c/ce383ba615339f8eaec646a166d2c2b015bb5ca0
- https://security-tracker.debian.org/tracker/CVE-2026-31696
- https://access.redhat.com/security/cve/cve-2026-31696
- https://bdu.fstec.ru/vul/2026-08757

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31680
BDU:2026-08794

Идентификатор программной ошибки: CWE-825 Разыменование недействительного указателя

Уязвимый продукт: Linux: от 6.19 до 6.19.12
Red Hat Enterprise Linux: 10
Debian GNU/Linux: 13

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.

36

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026042544-CVE-2026-31680-7624@gregkh/
- https://git.kernel.org/stable/c/4b6798024f7b2d535f3db1002c760143cdbd1bd3
- https://git.kernel.org/stable/c/3c54b66c83fb8fcbde8e6a7bf90b65856e39f827
- https://git.kernel.org/stable/c/5a6b15f861b7c1304949e3350d23490a5fe429fd
- https://git.kernel.org/stable/c/6c7fbdb8ffde6413640de7cfbd7c976c353e89f8
- https://git.kernel.org/stable/c/8027964931785cb73d520ac70a342a3dc16c249b
- https://git.kernel.org/stable/c/414726b69921fe6355ae453f5b35e68dd078342a
- https://git.kernel.org/stable/c/572ce62778519a7d4d1c15f55dd2e45a474133c4
- https://git.kernel.org/stable/c/9ca562bb8e66978b53028fa32b1a190708e6a091

- https://security-tracker.debian.org/tracker/CVE-2026-31680
- https://access.redhat.com/security/cve/cve-2026-31680
- https://vuldb.com/vuln/359585
- https://bdu.fstec.ru/vul/2026-08794

37

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31683
BDU:2026-08799

Идентификатор программной ошибки: CWE-131 Некорректный расчет размера буфера

Уязвимый продукт: Linux: от 2.6.38 до 5.10.253
Debian GNU/Linux: 13

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026042545-CVE-2026-31683-b833@gregkh/
- https://git.kernel.org/stable/c/67176c96f325837b0bb3e9538ca2eba414f447d8
- https://git.kernel.org/stable/c/0b10a8b355c3f71012ce89289ec2c2f5e3bfd6c1
- https://git.kernel.org/stable/c/6755347c5f9bdd44dee80f692208b056fcd40a52
- https://git.kernel.org/stable/c/1ada20331f2df2a942d6b83ae1f04a304b642e2a
- https://git.kernel.org/stable/c/6e40ebb999c2c3d2fbb3cacb61f0384ee6e69075
- https://git.kernel.org/stable/c/0e35db29fc5a97a8553f7c2d3a2ba730e46b1ee8
- https://git.kernel.org/stable/c/eda89a1bae0602aec8314ced299bb243b9f9aeef
- https://git.kernel.org/stable/c/0d4aef630be9d5f9c1227d07669c26c4383b5ad0
- https://security-tracker.debian.org/tracker/CVE-2026-31683

- https://access.redhat.com/security/cve/cve-2026-31683
- https://bdu.fstec.ru/vul/2026-08799

38

Краткое описание: Выполнение произвольного кода в Gogs

Идентификатор уязвимости: CVE-2026-52813
BDU:2026-08780

Идентификатор программной ошибки: CWE-23 Подмена относительного пути

Уязвимый продукт: Gogs: до 0.14.3

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:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-26 / 2026-06-26

Ссылки на источник:

- https://github.com/gogs/gogs/releases/tag/v0.14.3
- https://github.com/gogs/gogs/security/advisories/GHSA-c39w-43gm-34h5
- https://github.com/gogs/gogs/commit/f6acd467305943aae8403cbac81f0118dd1235d7
- https://github.com/gogs/gogs/pull/8334
- https://dailycve.com/gogs-path-traversal-vulnerability-leading-to-remote-code-execution-cve-2026-52813-critical-dc-jun2026-581/
- https://bdu.fstec.ru/vul/2026-08780

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-31685
BDU:2026-08760

Идентификатор программной ошибки: CWE-1012 Сквозные уязвимости

Уязвимый продукт: Linux: от 2.6.12 до 6.12.83
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Debian GNU/Linux: 13

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.

39

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026042545-CVE-2026-31685-3fcc@gregkh/
- https://git.kernel.org/stable/c/9eda5478746ef7dc0e4e537b5a5e4b0ca1027091
- https://git.kernel.org/stable/c/807d6ee15804df6f01a35c910f09612e858739a6
- https://git.kernel.org/stable/c/309ae3e9a51a69699ca94eac5fac5688fa562d55
- https://git.kernel.org/stable/c/fdce0b3590f724540795b874b4c8850c90e6b0a8
- https://security-tracker.debian.org/tracker/CVE-2026-31685
- https://access.redhat.com/security/cve/cve-2026-31685
- https://vuldb.com/vuln/359587
- https://bdu.fstec.ru/vul/2026-08760

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2025-71089
BDU:2026-08859

Идентификатор программной ошибки: CWE-820 Отсутствие синхронизации

Уязвимый продукт: Linux: от 5.2 до 6.12.63 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Debian GNU/Linux: 13

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.

40

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2025-71089
- https://git.kernel.org/stable/c/240cd7f2812cc25496b12063d11c823618f364e9
- https://git.kernel.org/stable/c/c2c3f1a3fd74ef16cf115f0c558616a13a8471b4
- https://git.kernel.org/stable/c/c341dee80b5df49a936182341b36395c831c2661
- https://git.kernel.org/linus/72f98ef9a4be30d2a60136dd6faee376f780d06c
- https://security-tracker.debian.org/tracker/CVE-2025-71089
- https://access.redhat.com/security/cve/cve-2025-71089
- https://bdu.fstec.ru/vul/2026-08859

41

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2025-71159
BDU:2026-08875

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.18 до 6.18.5 включительно

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://git.kernel.org/linus/83f59076a1ae6f5c6845d6f7ed3a1a373d883684
- https://www.cve.org/CVERecord?id=CVE-2025-71159
- https://git.kernel.org/stable/c/c8385851a5435f4006281828d428e5d0b0bbf8af
- https://lore.kernel.org/linux-cve-announce/2026012346-CVE-2025-71159-417a@gregkh/
- https://bdu.fstec.ru/vul/2026-08875

42

Краткое описание: Потеря целостности в Microsoft Edge

Идентификатор уязвимости: CVE-2026-32208
BDU:2026-08906

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

Уязвимый продукт: Microsoft Edge: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Потеря целостности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В 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: 2026-06-26 / 2026-06-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32208
- https://bdu.fstec.ru/vul/2026-08906

43

Краткое описание: Повышение привилегий в Microsoft Exchange Online

Идентификатор уязвимости: CVE-2026-48582
BDU:2026-08905

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Microsoft Exchange Online: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 9.6 AV:N/AC:L/PR:L/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: 2026-06-26 / 2026-06-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-48582
- https://bdu.fstec.ru/vul/2026-08905

44

Краткое описание: Повышение привилегий в Microsoft Dynamics 365

Идентификатор уязвимости: CVE-2026-47647
BDU:2026-08903

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Microsoft Dynamics 365: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 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: 2026-06-26 / 2026-06-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47647
- https://bdu.fstec.ru/vul/2026-08903

45

Краткое описание: Повышение привилегий в Linux

Идентификатор уязвимости: CVE-2026-43503
BDU:2026-08879

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

Уязвимый продукт: Linux: от 7.0 до 7.0.10
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Amazon Linux 2: Kernel-5.4 Extra
Amazon Linux: 2023

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

Способ эксплуатации: Манипулирование сроками и состоянием.

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:L/AC:L/PR:L/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: 2026-06-29 / 2026-06-29

Ссылки на источник:

- https://research.jfrog.com/post/dissecting-and-exploiting-linux-lpe-variant-dirtyclone-cve-2026-43503/
- https://lore.kernel.org/linux-cve-announce/2026052309-CVE-2026-43503-b134@gregkh/
- https://git.kernel.org/stable/c/3599e6b3cc1ada96883d496a50a210d3afbb6987
- https://git.kernel.org/stable/c/2f2b16022a2e10ca7bccfb98db5ed2ec0f72641c
- https://git.kernel.org/stable/c/9d3e5fd19fe1063bf607219e8562fbd567b8e8d5
- https://git.kernel.org/stable/c/78bf6b6bb19541d19fbda6242e7cfe2c682763c0

- https://git.kernel.org/stable/c/760e1addc27ba1a7beb4a0a7e8b3e9ec49e7a34e
- https://git.kernel.org/stable/c/3bd9e113d50034db99d7ef69fd8e5242d15e414a
- https://git.kernel.org/stable/c/3884358a9286b17f389a72b1426fc4547c23c111
- https://git.kernel.org/stable/c/f84eca5817390257cef78013d0112481c503b4a3
- https://explore.alas.aws.amazon.com/CVE-2026-43503.html
- https://ubuntu.com/security/CVE-2026-43503
- https://access.redhat.com/security/cve/cve-2026-43503
- https://security-tracker.debian.org/tracker/CVE-2026-43503
- https://www.penligent.ai/hackinglabs/cve-2026-43503-poc/
- https://nvd.nist.gov/vuln/detail/CVE-2026-43503
- https://bdu.fstec.ru/vul/2026-08879

46

Краткое описание: Выполнение произвольного кода в Oracle HTTP Server

Идентификатор уязвимости: CVE-2026-34291
BDU:2026-08897

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: HTTP Server: 14.1.2.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.7 AV:N/AC:H/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: 2026-04-27 / 2026-04-27

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpuapr2026.html
- https://bdu.fstec.ru/vul/2026-08897

47

Краткое описание: Выполнение произвольного кода в Financial Services Analytical Applications Infrastructure

Идентификатор уязвимости: CVE-2026-22010
BDU:2026-08896

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Financial Services Analytical Applications Infrastructure: 8.1.2.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpuapr2026.html
- https://bdu.fstec.ru/vul/2026-08896

48

Краткое описание: Выполнение произвольного кода в Application Development Framework

Идентификатор уязвимости: CVE-2026-35243
BDU:2026-08895

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Application Development Framework: 12.2.1.4.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpuapr2026.html
- https://bdu.fstec.ru/vul/2026-08895

49

Краткое описание: Отказ в обслуживании в Red Hat Enterprise Linux

Идентификатор уязвимости: CVE-2026-1519
BDU:2026-08885

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

Уязвимый продукт: Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Ubuntu: 25.10
BIND: от 9.21.0 до 9.21.20
Debian GNU/Linux: 13
Red Hat OpenShift Container Platform: 4

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: 2026-06-29 / 2026-06-29

Ссылки на источник:

- https://kb.isc.org/docs/cve-2026-1519
- https://downloads.isc.org/isc/bind9/9.18.47
- https://downloads.isc.org/isc/bind9/9.20.21
- https://downloads.isc.org/isc/bind9/9.21.20
- https://access.redhat.com/security/cve/cve-2026-1519
- https://security-tracker.debian.org/tracker/CVE-2026-1519
- https://ubuntu.com/security/CVE-2026-1519

- https://bdu.fstec.ru/vul/2026-08885

50

Краткое описание: Повышение привилегий в Microsoft 365 Copilot

Идентификатор уязвимости: CVE-2026-47645
BDU:2026-08882

Идентификатор программной ошибки: CWE-601 Перенаправление на небезопасный сайт ("открытое перенаправление")

Уязвимый продукт: Microsoft 365 Copilot: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

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: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: 2026-06-26 / 2026-06-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47645
- https://bdu.fstec.ru/vul/2026-08882

Краткое описание: Выполнение произвольного кода в Financial Services Transaction Filtering

Идентификатор уязвимости: CVE-2026-35231
BDU:2026-08891

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Financial Services Transaction Filtering: 8.1.2.8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-24 / 2026-04-24

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpuapr2026.html
- https://bdu.fstec.ru/vul/2026-08891

52

Краткое описание: Выполнение произвольного кода в Oracle Financial Services Customer Screening

Идентификатор уязвимости: CVE-2026-34320
BDU:2026-08893

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Oracle Financial Services Customer Screening: 8.1.2.8.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.oracle.com/security-alerts/cpuapr2026.html
- https://bdu.fstec.ru/vul/2026-08893

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43499
BDU:2026-08889

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 2.6.39 до 7.1-rc1
Debian GNU/Linux: 13
openSUSE Tumbleweed: -

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.

53

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-09 / 2026-02-09

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026052158-CVE-2026-43499-1294@gregkh/T/#u
- https://git.kernel.org/stable/c/3bfdc63936dd4773109b7b8c280c0f3b5ae7d349
- https://git.kernel.org/stable/c/3fb7394a837740770f0d6b4b30567e60786a63f2
- https://git.kernel.org/stable/c/6d52dfcb2a5db86e346cf51f8fcf2071b8085166
- https://git.kernel.org/stable/c/88614876370aac8ad1050ad785a4c095ba17ac11
- https://git.kernel.org/stable/c/8a1fc8d698ac5e5916e3082a0f74450d71f9611f
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-42456
- https://www.suse.com/security/cve/CVE-2026-43499.html
- https://security-tracker.debian.org/tracker/CVE-2026-43499

- https://github.com/MobiusM/CVE-2026-43499
- https://bdu.fstec.ru/vul/2026-08889

54

Краткое описание: Повышение привилегий в SINEC INS

Идентификатор уязвимости: CVE-2026-46748
BDU:2026-08948

Идентификатор программной ошибки: CWE-250 Выполнение операций с избыточными привилегиями

Уязвимый продукт: SINEC INS: до 1.0 SP2 Update 6

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-23 / 2026-06-23

Ссылки на источник:

- https://support.industry.siemens.com/cs/document/110002283/sinec-ins-v1-0-service-pack-2-update-6-software-(incl-10-node-demo)-%E2%80%93-download?dti=0&lc=en-CH
- https://bdu.fstec.ru/vul/2026-08948

55

Краткое описание: Обход безопасности в Apache Shiro

Идентификатор уязвимости: CVE-2026-49268
BDU:2026-08941

Идентификатор программной ошибки: CWE-90 Некорректная нейтрализация специальных элементов, используемых в LDAP-запросах (внедрение LDAP)

Уязвимый продукт: Shiro: от 3.0.0-alpha-0 до 3.0.0-alpha-1 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-30 / 2026-06-30

Ссылки на источник:

- http://www.openwall.com/lists/oss-security/2026/06/17/8
- https://lists.apache.org/thread/svszql3od8td7hn6conyj2oq70v53b5s
- https://bdu.fstec.ru/vul/2026-08941

56

Краткое описание: Потеря целостности в Apache APISIX

Идентификатор уязвимости: CVE-2026-49871
BDU:2026-08935

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

Уязвимый продукт: APISIX: от 3.0.0 до 3.16.0 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Потеря целостности

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-30 / 2026-06-30

Ссылки на источник:

- http://www.openwall.com/lists/oss-security/2026/06/19/14
- https://lists.apache.org/thread/1ozsnss0lof4gpwq763d66oxwxt3sycp
- https://bdu.fstec.ru/vul/2026-08935

57

Краткое описание: Повышение привилегий в Azure Active Directory (AAD)

Идентификатор уязвимости: CVE-2026-45480
BDU:2026-08927

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Azure Active Directory (AAD): -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-26 / 2026-06-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45480
- https://bdu.fstec.ru/vul/2026-08927

58

Краткое описание: Отказ в обслуживании в Cisco

Идентификатор уязвимости: CVE-2026-20103
BDU:2026-08921

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

Уязвимый продукт: Adaptive Security Appliance: 9.23.1.3
Cisco Secure Firewall Threat Defense (FTD): 6.4.0

Категория уязвимого продукта: Программно-аппаратное решение

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: 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: 2026-06-17 / 2026-06-17

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-m9sx6MbC
- https://bdu.fstec.ru/vul/2026-08921

59

Краткое описание: Обход безопасности в Apache APISIX

Идентификатор уязвимости: CVE-2026-39999
BDU:2026-08920

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

Уязвимый продукт: APISIX: от 2.12.0 до 3.16.0 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-30 / 2026-06-30

Ссылки на источник:

- http://www.openwall.com/lists/oss-security/2026/06/19/5
- https://lists.apache.org/thread/nfopt8cnxd3k0rs1oxtr7lzxrdw4mojq
- https://bdu.fstec.ru/vul/2026-08920

60

Краткое описание: Обход безопасности в Apache APISIX

Идентификатор уязвимости: CVE-2026-39998
BDU:2026-08919

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: APISIX: от 2.12.0 до 3.16.0 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

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: 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: 2026-06-30 / 2026-06-30

Ссылки на источник:

- http://www.openwall.com/lists/oss-security/2026/06/19/4
- https://lists.apache.org/thread/vgkvy396010d7g6m0jrn4d3hjf2svlvv
- https://bdu.fstec.ru/vul/2026-08919

61

Краткое описание: Выполнение произвольного кода в JetBrains Hub

Идентификатор уязвимости: CVE-2026-56141
BDU:2026-08916

Идентификатор программной ошибки: CWE-338 Использование ненадежного ГПСЧ

Уязвимый продукт: Hub: до 2026.1.13757

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-06-30 / 2026-06-30

Ссылки на источник:

- https://www.jetbrains.com/privacy-security/issues-fixed/
- https://bdu.fstec.ru/vul/2026-08916

62

Краткое описание: Повышение привилегий в Gitea

Идентификатор уязвимости: CVE-2026-58053
BDU:2026-08914

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Gitea: до 0.262.0 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 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: 2026-06-30 / 2026-06-30

Ссылки на источник:

- https://github.com/bikini/exploitarium/tree/main/gitea-act-runner-container-options-poc
- https://www.facebook.com/groups/349914115877020/posts/2095861054615642/
- https://www.vulncheck.com/advisories/gitea-act-runner-container-hardening-bypass-via-workflow-container-options
- https://bdu.fstec.ru/vul/2026-08914

63

Краткое описание: Выполнение произвольного кода в babel

Идентификатор уязвимости: CVE-2026-44728
BDU:2026-08998

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

Уязвимый продукт: babel: от 8.0.0-alpha.0 до 8.0.0-alpha.13

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-01 / 2026-06-01

Ссылки на источник:

- https://github.com/babel/babel/security/advisories/GHSA-fv7c-fp4j-7gwp
- https://bdu.fstec.ru/vul/2026-08998

64

Краткое описание: Выполнение произвольного кода в Simcenter Femap

Идентификатор уязвимости: CVE-2025-12659
BDU:2026-09001

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

Уязвимый продукт: Simcenter Femap: до 2512.0003

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-20 / 2026-05-20

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-870926.html
- https://bdu.fstec.ru/vul/2026-09001

65

Краткое описание: Получение конфиденциальной информации в Siemens Teamcenter

Идентификатор уязвимости: CVE-2026-33893
BDU:2026-09018

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: Siemens Teamcenter: до 2506.0005

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-20 / 2026-05-20

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-827383.html
- https://bdu.fstec.ru/vul/2026-09018

66

Краткое описание: Получение конфиденциальной информации в Grafana

Идентификатор уязвимости: CVE-2026-27877
BDU:2026-08995

Идентификатор программной ошибки: CWE-312 Хранение важных данных в незашифрованном виде

Уязвимый продукт: Red Hat Enterprise Linux: 10.0 Extended Update Support
РЕД ОС: 8.0
Grafana: от 12.3.6 до 12.4.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-09 / 2026-06-09

Ссылки на источник:

- https://github.com/advisories/GHSA-3q27-7qjq-p9c5
- https://github.com/grafana/grafana
- https://grafana.com/security/security-advisories/cve-2026-27877
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-27877
- https://access.redhat.com/security/cve/cve-2026-27877
- https://bdu.fstec.ru/vul/2026-08995

67

Краткое описание: Повышение привилегий в Libxml2

Идентификатор уязвимости: CVE-2024-34459
BDU:2026-08991

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

Уязвимый продукт: Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Ubuntu: 24.04 LTS
libxml2: до 2.12.7
Debian GNU/Linux: 12
РЕД ОС: 7.3
Amazon Linux 2: Core
Amazon Linux: 2023
Discovery: 2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://gitlab.gnome.org/GNOME/libxml2/-/releases/v2.12.7
- https://gitlab.gnome.org/GNOME/libxml2/-/releases/v2.11.8
- https://gitlab.gnome.org/GNOME/libxml2/-/work_items/720
- https://redos.red-soft.ru/support/secure/uyazvimosti/uyazvimost-libxml2-cve-2024-34459/

- https://ubuntu.com/security/CVE-2024-34459
- https://explore.alas.aws.amazon.com/CVE-2024-34459.html
- https://access.redhat.com/security/cve/cve-2024-34459
- https://security-tracker.debian.org/tracker/CVE-2024-34459
- https://bdu.fstec.ru/vul/2026-08991

68

Краткое описание: Выполнение произвольного кода в E-Business Suite

Идентификатор уязвимости: CVE-2026-46817
BDU:2026-08976

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

Уязвимый продукт: E-Business Suite: от 12.2.3 до 12.2.15 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 9.8 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: 2026-06-30 / 2026-06-30

Ссылки на источник:

- https://securityaffairs.com/194463/security/attackers-actively-exploit-the-oracle-e-business-suite-flaw-cve-2026-46817.html
- https://www.oracle.com/security-alerts/cspumay2026.html
- https://thehackernews.com/2026/06/oracle-e-business-suite-flaw-cve-2026.html
- https://www.helpnetsecurity.com/2026/06/30/oracle-payments-cve-2026-46817-exploitation/
- https://bdu.fstec.ru/vul/2026-08976

69

Краткое описание: Выполнение произвольного кода в Gitlab

Идентификатор уязвимости: CVE-2026-10712
BDU:2026-08984

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

Уязвимый продукт: Gitlab: от 19.1 до 19.1.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-1-1-released/
- https://bdu.fstec.ru/vul/2026-08984

70

Краткое описание: Получение конфиденциальной информации в Gitlab

Идентификатор уязвимости: CVE-2026-12053
BDU:2026-08986

Идентификатор программной ошибки: CWE-532 Включение важной информации в файлы журналов

Уязвимый продукт: Gitlab: от 19.1 до 19.1.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Несанкционированный сбор информации.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-1-1-released/
- https://bdu.fstec.ru/vul/2026-08986

71

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-10911
BDU:2026-09174

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: до 149.0.7827.54
Microsoft Edge: до 149.0.4022.52

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

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: 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: 2026-07-02 / 2026-07-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://feedly.com/cve/CVE-2026-10911
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-10911
- https://bdu.fstec.ru/vul/2026-09174

72

Краткое описание: Выполнение произвольного кода в ColdFusion

Идентификатор уязвимости: CVE-2026-48281
BDU:2026-09170

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: ColdFusion: 2023 до Update 21

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:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-53902
- https://bdu.fstec.ru/vul/2026-09170

73

Краткое описание: Выполнение произвольного кода в ColdFusion

Идентификатор уязвимости: CVE-2026-48277
BDU:2026-09169

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: ColdFusion: 2023 до Update 21

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:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-53901
- https://bdu.fstec.ru/vul/2026-09169

74

Краткое описание: Отказ в обслуживании в Google Chrome

Идентификатор уязвимости: CVE-2026-11024
BDU:2026-09157

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Google Chrome: до 149.0.7827.53

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-46553
- https://bdu.fstec.ru/vul/2026-09157

75

Краткое описание: Выполнение произвольного кода в ColdFusion

Идентификатор уязвимости: CVE-2026-48316
BDU:2026-09167

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: ColdFusion: 2023 до Update 21

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:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html
- https://bdu.fstec.ru/vul/2026-09167

76

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-10907
BDU:2026-09176

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Google Chrome: до 149.0.7827.54
Microsoft Edge: до 149.0.4022.52

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: 2026-07-02 / 2026-07-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://feedly.com/cve/CVE-2026-10907
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10907
- https://bdu.fstec.ru/vul/2026-09176

77

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-10937
BDU:2026-09185

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

Уязвимый продукт: Google Chrome: до 149.0.7827.54
Microsoft Edge: до 149.0.4022.52

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-02 / 2026-07-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-10937
- https://feedly.com/cve/CVE-2026-10937
- https://bdu.fstec.ru/vul/2026-09185

78

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-10947
BDU:2026-09184

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.54
Microsoft Edge: до 149.0.4022.52

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-02 / 2026-07-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-10947
- https://bdu.fstec.ru/vul/2026-09184

79

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-10929
BDU:2026-09182

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

Уязвимый продукт: Google Chrome: до 149.0.7827.53
Microsoft Edge: до 149.0.4022.53

Категория уязвимого продукта: Прикладное программное обеспечение

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.

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: 2026-07-02 / 2026-07-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-10929
- https://bdu.fstec.ru/vul/2026-09182

80

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-10938
BDU:2026-09181

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: до 149.0.7827.54
Microsoft Edge: до 149.0.4022.52

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-02 / 2026-07-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-10938
- https://bdu.fstec.ru/vul/2026-09181

81

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-10882
BDU:2026-09092

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.54
Microsoft Edge: до 149.0.4022.52

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-02 / 2026-07-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2026-10882
- https://bdu.fstec.ru/vul/2026-09092

82

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-11019
BDU:2026-09142

Идентификатор программной ошибки: CWE-451 Некорректное представление важной информации интерфейсом пользователя

Уязвимый продукт: Google Chrome: до 149.0.7827.53

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-46548
- https://bdu.fstec.ru/vul/2026-09142

83

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-11010
BDU:2026-09099

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.53

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-46539
- https://bdu.fstec.ru/vul/2026-09099

84

Краткое описание: Отказ в обслуживании в Next.js

Идентификатор уязвимости: CVE-2026-44577
BDU:2026-09098

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

Уязвимый продукт: Red Hat Enterprise Linux: 10
Next.js: до 16.2.5
Red Hat Enterprise Linux AI: 3
Red Hat Trusted Artifact Signer: -
Streams for Apache Kafka: 3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-29 / 2026-06-29

Ссылки на источник:

- https://github.com/vercel/next.js/security/advisories/GHSA-h64f-5h5j-jqjh
- https://access.redhat.com/security/cve/cve-2026-44577
- https://bdu.fstec.ru/vul/2026-09098

85

Краткое описание: Отказ в обслуживании в Next.js

Идентификатор уязвимости: CVE-2026-44579
BDU:2026-09096

Идентификатор программной ошибки: CWE-833 Взаимоблокировка

Уязвимый продукт: Next.js: до 16.2.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-29 / 2026-06-29

Ссылки на источник:

- https://github.com/vercel/next.js/security/advisories/GHSA-mg66-mrh9-m8jx
- https://bdu.fstec.ru/vul/2026-09096

86

Краткое описание: Получение конфиденциальной информации в Next.js

Идентификатор уязвимости: CVE-2026-44575
BDU:2026-09095

Идентификатор программной ошибки: CWE-551 Некорректный порядок действий: авторизация до обработки и нормализации

Уязвимый продукт: Red Hat Enterprise Linux: 10
Next.js: до 16.2.5
Red Hat Enterprise Linux AI: 3
Red Hat Trusted Artifact Signer: -
Streams for Apache Kafka: 3

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-29 / 2026-06-29

Ссылки на источник:

- https://github.com/vercel/next.js/security/advisories/GHSA-267c-6grr-h53f
- https://access.redhat.com/security/cve/cve-2026-44575
- https://bdu.fstec.ru/vul/2026-09095

87

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-11040
BDU:2026-09094

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.53

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-46569
- https://bdu.fstec.ru/vul/2026-09094

88

Краткое описание: Отказ в обслуживании в protobufjs

Идентификатор уязвимости: CVE-2026-44290
BDU:2026-09088

Идентификатор программной ошибки: CWE-1008 Архитектурные принципы

Уязвимый продукт: protobufjs: от 8.0.0 до 8.0.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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: 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: 2026-06-29 / 2026-06-29

Ссылки на источник:

- https://github.com/protobufjs/protobuf.js/security/advisories/GHSA-jvwf-75h9-cwgg
- https://bdu.fstec.ru/vul/2026-09088

89

Краткое описание: Выполнение произвольного кода в GitHub Copilot

Идентификатор уязвимости: CVE-2026-45033
BDU:2026-09077

Идентификатор программной ошибки: CWE-696 Некорректный порядок работы

Уязвимый продукт: GitHub Copilot: до 1.0.43

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2026-06-30 / 2026-06-30

Ссылки на источник:

- https://github.com/github/copilot-cli/security/advisories/GHSA-9ccr-r5hg-74gf
- https://bdu.fstec.ru/vul/2026-09077

90

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: VE-2026-11000
BDU:2026-09106

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.53

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-46529
- https://bdu.fstec.ru/vul/2026-09106

91

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-11002
BDU:2026-09102

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.53

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-46531
- https://bdu.fstec.ru/vul/2026-09102

92

Краткое описание: Выполнение произвольного кода в protobufjs

Идентификатор уязвимости: CVE-2026-44293
BDU:2026-09109

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

Уязвимый продукт: Red Hat Enterprise Linux: 9
OpenShift Container Platform: 4
Openshift Service Mesh: 3.3
Red Hat Openshift Data Foundation: 4
Red Hat Ansible Automation Platform: 2
OpenShift Pipelines: -
Red Hat Developer Hub: 1.9
Red Hat Enterprise Linux AI: 3
Red Hat Hardened Images: -
protobufjs: от 8.0.0 до 8.0.2
Red Hat Build of Podman Desktop: -
Self-service automation portal: 2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-06-29 / 2026-06-29

Ссылки на источник:

- https://github.com/protobufjs/protobuf.js/security/advisories/GHSA-66ff-xgx4-vchm
- https://access.redhat.com/security/cve/cve-2026-44293
- https://bdu.fstec.ru/vul/2026-09109

93

Краткое описание: Получение конфиденциальной информации в Znuny

Идентификатор уязвимости: CVE-2025-26842
BDU:2026-09141

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: Znuny: 6.0 LTS

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-03-06 / 2025-03-06

Ссылки на источник:

- https://security-tracker.debian.org/tracker/CVE-2025-26842
- https://www.znuny.org/en/advisories/zsa-2025-01
- https://bdu.fstec.ru/vul/2026-09141

94

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-11041
BDU:2026-09133

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: до 149.0.7827.53

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-46570
- https://bdu.fstec.ru/vul/2026-09133

95

Краткое описание: Отказ в обслуживании в protobufjs

Идентификатор уязвимости: CVE-2026-44289
BDU:2026-09107

Идентификатор программной ошибки: CWE-674 Неконтролируемая рекурсия

Уязвимый продукт: protobufjs: от 8.0.0 до 8.0.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-29 / 2026-06-29

Ссылки на источник:

- https://github.com/protobufjs/protobuf.js/security/advisories/GHSA-685m-2w69-288q
- https://www.sentinelone.com/vulnerability-database/cve-2026-44289/
- https://bdu.fstec.ru/vul/2026-09107

96

Краткое описание: Выполнение произвольного кода в pgAdmin 4

Идентификатор уязвимости: CVE-2026-7815
BDU:2026-09129

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

Уязвимый продукт: pgAdmin 4: до 9.15

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-01 / 2026-07-01

Ссылки на источник:

- Использование рекомендаций:
- https://github.com/pgadmin-org/pgadmin4/issues/9898
- https://bdu.fstec.ru/vul/2026-09129

97

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-10887
BDU:2026-09128

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.53

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-02 / 2026-07-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://bdu.fstec.ru/vul/2026-09128

98

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2026-11047
BDU:2026-09132

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Google Chrome: до 149.0.7827.53

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-46576
- https://bdu.fstec.ru/vul/2026-09132

99

Краткое описание: Перезапись произвольных файлов в pgAdmin 4

Идентификатор уязвимости: CVE-2026-7819
BDU:2026-09125

Идентификатор программной ошибки: CWE-61 Уязвимости, связанные с символическими ссылками UNIX

Уязвимый продукт: pgAdmin 4: до 9.15

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://www.cve.org/CVERecord?idCVE-2026-7819
- https://github.com/pgadmin-org/pgadmin4/issues/9902
- https://github.com/pgadmin-org/pgadmin4/commit/435752b83
- https://bdu.fstec.ru/vul/2026-09125

100

Краткое описание: Выполнение произвольного кода в pgAdmin 4

Идентификатор уязвимости: CVE-2026-7818
BDU:2026-09124

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: pgAdmin 4: до 9.15

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://www.cve.org/CVERecord?idCVE-2026-7818
- https://github.com/pgadmin-org/pgadmin4/issues/9901
- https://bdu.fstec.ru/vul/2026-09124

101

Краткое описание: Выполнение произвольного кода в pgAdmin 4

Идентификатор уязвимости: CVE-2026-7816
BDU:2026-09123

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

Уязвимый продукт: pgAdmin 4: до 9.15

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-07-01 / 2026-07-01

Ссылки на источник:

- https://www.cve.org/CVERecord?idCVE-2026-7816
- https://github.com/pgadmin-org/pgadmin4/issues/9899
- https://bdu.fstec.ru/vul/2026-09123

102

Краткое описание: Повышение привилегий в Dell Automation Platform

Идентификатор уязвимости: CVE-2026-32658
BDU:2026-09122

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Dell Automation Platform: до 2.0.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-06-23 / 2026-06-23

Ссылки на источник:

- https://www.cve.org/CVERecord?idCVE-2026-32658
- https://www.dell.com/support/kbdoc/en-us/000458049/dsa-2026-193-security-update-for-dell-automation-platform-multiple-vulnerabilities
- https://bdu.fstec.ru/vul/2026-09122

103

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-10885
BDU:2026-09113

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.53

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие специально созданной HTML-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-07-02 / 2026-07-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://bdu.fstec.ru/vul/2026-09113

104

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2026-10891
BDU:2026-09126

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome: до 149.0.7827.53

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: 2026-07-02 / 2026-07-02

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/06/stable-channel-update-for-desktop.html
- https://bdu.fstec.ru/vul/2026-09126

105

Краткое описание: Получение конфиденциальной информации в Microsoft Cost Management

Идентификатор уязвимости: CVE-2026-47633
BDU:2026-09145

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

Уязвимый продукт: Microsoft Cost Management: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-26 / 2026-06-26

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-47633
- https://bdu.fstec.ru/vul/2026-09145

Краткое описание: Отказ в обслуживании в Secure Endpoint Private Cloud

Идентификатор уязвимости: CVE-2026-20215
BDU:2026-09212

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

Уязвимый продукт: Secure Endpoint Private Cloud: до 4.2.8
Secure Endpoint Connector: до 8.6.2

Категория уязвимого продукта: Программно-аппаратное решение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Отказ в обслуживании

106 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-07-03 / 2026-07-03

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR
- https://bdu.fstec.ru/vul/2026-09212

Краткое описание: Отказ в обслуживании в Secure Endpoint Private Cloud

Идентификатор уязвимости: CVE-2026-20244
BDU:2026-09218

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

Уязвимый продукт: Secure Endpoint Private Cloud: до 4.2.8
Secure Endpoint Connector: до 8.6.2

Категория уязвимого продукта: Программно-аппаратное решение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Отказ в обслуживании

107 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-07-03 / 2026-07-03

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR
- https://bdu.fstec.ru/vul/2026-09218

Краткое описание: Отказ в обслуживании в Secure Endpoint Private Cloud

Идентификатор уязвимости: CVE-2026-20243
BDU:2026-09214

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

Уязвимый продукт: Secure Endpoint Private Cloud: до 4.2.8
Secure Endpoint Connector: до 8.6.2

Категория уязвимого продукта: Программно-аппаратное решение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Отказ в обслуживании

108 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-07-03 / 2026-07-03

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR
- https://bdu.fstec.ru/vul/2026-09214

Краткое описание: Отказ в обслуживании в Secure Endpoint Private Cloud

Идентификатор уязвимости: CVE-2026-20217
BDU:2026-09213

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

Уязвимый продукт: Secure Endpoint Private Cloud: до 4.2.8
Secure Endpoint Connector: до 8.6.2

Категория уязвимого продукта: Программно-аппаратное решение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Отказ в обслуживании

109 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-07-03 / 2026-07-03

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR
- https://bdu.fstec.ru/vul/2026-09213

Краткое описание: Отказ в обслуживании в Secure Endpoint Private Cloud

Идентификатор уязвимости: CVE-2026-20214
BDU:2026-09210

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

Уязвимый продукт: Secure Endpoint Private Cloud: до 4.2.8
Secure Endpoint Connector: до 8.6.2

Категория уязвимого продукта: Программно-аппаратное решение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Отказ в обслуживании

110 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-07-03 / 2026-07-03

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR
- https://bdu.fstec.ru/vul/2026-09210

111

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2025-39793
BDU:2026-09206

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

Уязвимый продукт: Linux: от 6.14 до 6.15.10 включительно
Red Hat Enterprise Linux: 10

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

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-02-11 / 2026-02-11

Ссылки на источник:

- https://www.cve.org/CVERecord?id=CVE-2025-39793
- https://git.kernel.org/stable/c/c6a2706e08b8a1b2d3740161c0977d38e596c1ee
- https://git.kernel.org/stable/c/a69a9b53c54e2d33e2a5b1ea4a9a71fd01c6cf3a
- https://git.kernel.org/linus/33503c083fda048c77903460ac0429e1e2c0e341
- https://kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.15.11
- https://kernel.org/pub/linux/kernel/v6.x/ChangeLog-6.16.2
- https://lore.kernel.org/linux-cve-announce/2025091223-CVE-2025-39793-9d74@gregkh/
- https://access.redhat.com/security/cve/cve-2025-39793
- https://bdu.fstec.ru/vul/2026-09206

112

Краткое описание: Выполнение произвольного кода в Trust Protection Foundation

Идентификатор уязвимости: CVE-2026-0241
BDU:2026-09201

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

Уязвимый продукт: Trust Protection Foundation: от 24.1.0 до 24.1.13

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 8.6 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: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://security.paloaltonetworks.com/CVE-2026-0241
- https://security.paloaltonetworks.com/?sort=-updated
- https://www.cybersecurity-help.cz/vdb/SB2026051460
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-40766
- https://bdu.fstec.ru/vul/2026-09201

Краткое описание: Повышение привилегий в VMware Fusion

Идентификатор уязвимости: CVE-2026-41702
BDU:2026-09200

Идентификатор программной ошибки: CWE-367 Состояние гонки, связанное со временем проверки и временем использования

Уязвимый продукт: VMware Fusion: до 26h1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование сроками и состоянием.

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.

113

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-20 / 2026-05-20

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/37454
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-40932
- https://www.cybersecurity-help.cz/vdb/SB2026051468
- https://bdu.fstec.ru/vul/2026-09200

Краткое описание: Отказ в обслуживании в Secure Endpoint Private Cloud

Идентификатор уязвимости: CVE-2026-20213
BDU:2026-09209

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

Уязвимый продукт: Secure Endpoint Private Cloud: до 4.2.8
Secure Endpoint Connector: до 8.6.2

Категория уязвимого продукта: Программно-аппаратное решение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Отказ в обслуживании

114 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-07-03 / 2026-07-03

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-88cFYyxR
- https://bdu.fstec.ru/vul/2026-09209

115

Краткое описание: Выполнение произвольного кода в ColdFusion

Идентификатор уязвимости: CVE-2026-48307
BDU:2026-09262

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

Уязвимый продукт: ColdFusion: 2023 до Update 21

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-10 / 2025-12-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-53907
- https://bdu.fstec.ru/vul/2026-09262

116

Краткое описание: Чтение локальных файлов в ColdFusion

Идентификатор уязвимости: CVE-2026-48285
BDU:2026-09263

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

Уязвимый продукт: ColdFusion: 2023 до Update 21

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-11 / 2025-07-11

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-53905
- https://bdu.fstec.ru/vul/2026-09263

Краткое описание: Отказ в обслуживании в Python

Идентификатор уязвимости: CVE-2026-44432
BDU:2026-09264

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

Уязвимый продукт: urllib3: от 2.6.0 до 2.7.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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.

117

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: 2026-06-29 / 2026-06-29

Ссылки на источник:

- https://github.com/urllib3/urllib3/security/advisories/GHSA-mf9v-mfxr-j63j
- https://feedly.com/cve/CVE-2026-44432
- https://access.redhat.com/security/cve/cve-2026-44432
- https://ubuntu.com/security/CVE-2026-44432
- https://bdu.fstec.ru/vul/2026-09264

118

Краткое описание: Получение конфиденциальной информации в Mattermost

Идентификатор уязвимости: CVE-2026-4858
BDU:2026-09267

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

Уязвимый продукт: Mattermost: 11.6.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

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: 9.9 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: 2025-02-26 / 2025-02-26

Ссылки на источник:

- https://mattermost.com/security-updates
- https://threataft.com/articles/mattermost-cve-2026-4858-path-traversal-api-takeover
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-42439
- https://osv.dev/vulnerability/GO-2026-5311
- https://bdu.fstec.ru/vul/2026-09267

119

Краткое описание: Выполнение произвольного кода в pgAdmin 4

Идентификатор уязвимости: CVE-2026-12046
BDU:2026-09272

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: pgAdmin 4: от 6.9 до 9.16

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://github.com/pgadmin-org/pgadmin4/issues/10072
- https://github.com/pgadmin-org/pgadmin4/commit/f81433ae2f998f95bb17f27f53b4e99ebcc1df9c
- https://bdu.fstec.ru/vul/2026-09272

120

Краткое описание: Отказ в обслуживании в Go

Идентификатор уязвимости: CVE-2026-42504
BDU:2026-09276

Идентификатор программной ошибки: CWE-407 Алгоритмическая сложность

Уязвимый продукт: Go: от 1.26.0-0 до 1.26.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-03 / 2026-07-03

Ссылки на источник:

- https://pkg.go.dev/vuln/GO-2026-5038
- https://groups.google.com/g/golang-announce/c/tKs3rmcBcKw
- https://bdu.fstec.ru/vul/2026-09276

121

Краткое описание: Отказ в обслуживании в Go

Идентификатор уязвимости: CVE-2026-27145
BDU:2026-09275

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

Уязвимый продукт: Go: от 1.26.0-0 до 1.26.4

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-03 / 2026-07-03

Ссылки на источник:

- https://pkg.go.dev/vuln/GO-2026-5037
- https://groups.google.com/g/golang-announce/c/tKs3rmcBcKw
- https://bdu.fstec.ru/vul/2026-09275

122

Краткое описание: Выполнение произвольного кода в Oracle Enterprise Command Center Framework

Идентификатор уязвимости: CVE-2026-46896
BDU:2026-09280

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Oracle Enterprise Command Center Framework: 16

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 9.1 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: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-09280

123

Краткое описание: Отказ в обслуживании в NetScaler Gateway

Идентификатор уязвимости: CVE-2026-8452
BDU:2026-09281

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

Уязвимый продукт: NetScaler Gateway: от 13.1 до 63.18
NetScaler ADC FIPS: от 13.1 до 37.272
NetScaler ADC NDcPP: от 13.1 до 37.272
NetScaler ADC: от 13.1 до 63.18

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604
- https://bdu.fstec.ru/vul/2026-09281

124

Краткое описание: Получение конфиденциальной информации в NetScaler Gateway

Идентификатор уязвимости: CVE-2026-10816
BDU:2026-09283

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

Уязвимый продукт: NetScaler Gateway: от 13.1 до 63.18
NetScaler ADC FIPS: от 13.1 до 37.272
NetScaler ADC NDcPP: от 13.1 до 37.272
NetScaler ADC: от 13.1 до 63.18

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX696604
- https://bdu.fstec.ru/vul/2026-09283

Краткое описание: Отказ в обслуживании в Eclipse Wakaama

Идентификатор уязвимости: CVE-2026-58465
BDU:2026-09284

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

Уязвимый продукт: Eclipse Wakaama: до snapshot/2026-05-26

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

125

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: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://github.com/eclipse-wakaama/wakaama/releases
- https://www.vulncheck.com/advisories/eclipse-wakaama-coap-block1-handler-unbounded-memory-allocation-dos
- https://github.com/eclipse-wakaama/wakaama/pull/881
- https://bdu.fstec.ru/vul/2026-09284

126

Краткое описание: Выполнение произвольного кода в SandboxJS

Идентификатор уязвимости: CVE-2026-43898
BDU:2026-09273

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

Уязвимый продукт: SandboxJS: до 0.9.6

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-06-29 / 2026-06-29

Ссылки на источник:

- https://github.com/nyariv/SandboxJS/commit/826865251232611ec94078bab5a18ec875dad4a5
- https://github.com/nyariv/SandboxJS/security/advisories/GHSA-g8f2-4f4f-5jqw
- https://bdu.fstec.ru/vul/2026-09273

127

Краткое описание: Выполнение произвольного кода в pgAdmin 4

Идентификатор уязвимости: CVE-2026-12045
BDU:2026-09256

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

Уязвимый продукт: pgAdmin 4: от 9.13 до 9.16

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.0 AV:N/AC:L/PR:L/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: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://github.com/pgadmin-org/pgadmin4/commit/bf4792444446f0e7ab721d23cbd6bfe6afaa7a8b
- https://github.com/pgadmin-org/pgadmin4/issues/10022
- https://bdu.fstec.ru/vul/2026-09256

128

Краткое описание: Получение конфиденциальной информации в Rancher

Идентификатор уязвимости: CVE-2026-41053
BDU:2026-09231

Идентификатор программной ошибки: CWE-303 Некорректная реализация алгоритма аутентификации

Уязвимый продукт: Rancher: от 2.13.0 до 2.13.6

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: 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: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://dailycve.com/rancher-manager-incorrect-authentication-caching-privilege-escalation-cve-2026-41053-high-dc-jul2026-794/
- https://github.com/rancher/rancher/security/advisories/GHSA-4j6x-2764-m8gh
- https://bdu.fstec.ru/vul/2026-09231

129

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46242
BDU:2026-09232

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.18 до 6.18.33
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Amazon Linux: 2023

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: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://lore.kernel.org/linux-cve-announce/2026053014-CVE-2026-46242-8394@gregkh/
- https://git.kernel.org/stable/c/ef4ca02e95363e78977ca04340d44fe3b4b2b81f
- https://git.kernel.org/stable/c/ced39b6a8062bac5c18a1c3df85634107eb8664a
- https://git.kernel.org/stable/c/a6dc643c69311677c574a0f17a3f4d66a5f3744b
- https://feedly.com/cve/CVE-2026-31431
- https://github.com/J-jaeyoung/bad-epoll
- https://access.redhat.com/security/cve/cve-2026-46242

- https://security-tracker.debian.org/tracker/CVE-2026-46242
- https://ubuntu.com/security/CVE-2026-46242
- https://explore.alas.aws.amazon.com/CVE-2026-46242.html
- https://bdu.fstec.ru/vul/2026-09232

Краткое описание: Чтение локальных файлов в Gitea

Идентификатор уязвимости: CVE-2026-22874
BDU:2026-09234

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

Уязвимый продукт: Gitea: до 1.26.3

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

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.

130

Оценка CVSSv3: 9.6 AV:N/AC:L/PR:L/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: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://github.com/go-gitea/gitea/security/advisories/GHSA-2r5c-gw76-rh3w
- https://blog.gitea.com/release-of-1.26.3-and-1.26.4/
- https://github.com/go-gitea/gitea/releases/tag/v1.26.3
- https://bdu.fstec.ru/vul/2026-09234

131

Краткое описание: Выполнение произвольного кода в ColdFusion

Идентификатор уязвимости: CVE-2026-48283
BDU:2026-09257

Идентификатор программной ошибки: CWE-434 Отсутствие ограничений на загрузку файлов небезопасного типа

Уязвимый продукт: ColdFusion: 2023 до Update 21

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-10 / 2025-12-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb26-68.html
- https://dbugs.ptsecurity.com/vulnerability/PT-2026-53904
- https://bdu.fstec.ru/vul/2026-09257

132

Краткое описание: Отказ в обслуживании в Hitachi Virtual Storage Platform G1000

Идентификатор уязвимости: CVE-2025-7737
BDU:2026-09242

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

Уязвимый продукт: Hitachi Virtual Storage Platform G1000: -
Hitachi Virtual Storage Platform G1500: -
Hitachi Virtual Storage Platform F1500: -
Hitachi Virtual Storage Platform 5100: -
Hitachi Virtual Storage Platform 5500: -
Hitachi Virtual Storage Platform 5100H: -
Hitachi Virtual Storage Platform 5500H: -
Hitachi Virtual Storage Platform 5200: -
Hitachi Virtual Storage Platform 5600: -
Hitachi Virtual Storage Platform 5200H: -
Hitachi Virtual Storage Platform 5600H: -
Hitachi Virtual Storage Platform G100: -
Hitachi Virtual Storage Platform G200: -
Hitachi Virtual Storage Platform G400: -
Hitachi Virtual Storage Platform G600: -
Hitachi Virtual Storage Platform G800: -
Hitachi Virtual Storage Platform F400: -
Hitachi Virtual Storage Platform F600: -
Hitachi Virtual Storage Platform G130: -
Hitachi Virtual Storage Platform G150: -
Hitachi Virtual Storage Platform G350: -
Hitachi Virtual Storage Platform G370: -
Hitachi Virtual Storage Platform G700: -
Hitachi Virtual Storage Platform G900: -
Hitachi Virtual Storage Platform E590: -
Hitachi Virtual Storage Platform E790: -
Hitachi Virtual Storage Platform E990: -
Hitachi Virtual Storage Platform E1090: -
Hitachi Virtual Storage Platform E590H: -

Hitachi Virtual Storage Platform E790H: -
Hitachi Virtual Storage Platform E1090H: -
Hitachi Virtual Storage Platform E390H: -
Hitachi Virtual Storage Platform VX7: -

Категория уязвимого продукта: Программно-аппаратное решение

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: 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: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://www.hitachi.com/products/it/storage-solutions/sec_info/2026/2026_312.html
- https://bdu.fstec.ru/vul/2026-09242

133

Краткое описание: Выполнение произвольного кода в E-Business Suite

Идентификатор уязвимости: CVE-2026-46915
BDU:2026-09245

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: E-Business Suite: от 12.2.3 до 12.2.15 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 8.5 AV:N/AC:H/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: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-09245

134

Краткое описание: Выполнение произвольного кода в E-Business Suite

Идентификатор уязвимости: CVE-2026-46927
BDU:2026-09246

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

Уязвимый продукт: E-Business Suite: от 12.2.3 до 12.2.15 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://www.oracle.com/security-alerts/cspujun2026.html
- https://bdu.fstec.ru/vul/2026-09246

135

Краткое описание: Отказ в обслуживании в Cisco Identity Services Engine

Идентификатор уязвимости: CVE-2026-20181
BDU:2026-09239

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

Уязвимый продукт: Cisco Identity Services Engine: от 3.5 до 3.5 Patch 4
Identity Services Engine Passive Identity Connector (ISE-PIC): от 3.5 до 3.5 Patch 4

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2026-07-06 / 2026-07-06

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-G5WP8vv
- https://bdu.fstec.ru/vul/2026-09239