НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-06-03.1 | 3 июня 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2026-48899	Joomla!	Сетевой	PE	2026-05-26	✓
2	Критическая	CVE-2026-48904	Joomla!	Сетевой	PE	2026-05-26	✓
3	Критическая	CVE-2026-48898	Joomla!	Сетевой	PE	2026-05-26	✓
4	Критическая	CVE-2026-44930	Apache CXF	Сетевой	OSI	2026-05-26	✓
5	Высокая	CVE-2026-44417	Apache CXF	Сетевой	ACE	2026-05-26	✓
6	Высокая	CVE-2025-67030	Codehaus plexus-utils	Сетевой	ACE	2026-05-26	✓
7	Высокая	CVE-2026-4775	LibTIFF	Локальный	DoS	2026-05-26	✓
8	Критическая	CVE-2026-8495	Date iCal module for Drupal	Сетевой	OSI	2026-05-26	✓
9	Критическая	CVE-2026-48172	LiteSpeed User-End cPanel Plugin	Сетевой	OSI	2026-05-25	✓
10	Высокая	CVE-2026-9256	NGINX ngx_http_rewrite_module module	Сетевой	ACE	2026-05-25	✓
11	Высокая	CVE-2026-5843	Docker Desktop	Локальный	ACE	2026-05-22	✓
12	Высокая	CVE-2026-5817	Docker Desktop	Локальный	ACE	2026-05-22	✓
13	Высокая	CVE-2026-41326	Kata Containers	Сетевой	OSI	2026-05-22	✓

14	Высокая	CVE-2026-3039	ISC BIND	Сетевой	DoS	2026-05-22	✓
15	Высокая	CVE-2026-5946	ISC BIND	Сетевой	DoS	2026-05-22	✓
16	Высокая	CVE-2026-5947	ISC BIND	Сетевой	DoS	2026-05-22	✓
17	Высокая	CVE-2026-9089	ConnectWise Automate	Смежная сеть	ACE	2026-05-21	✓
18	Критическая	CVE-2026-20223	Cisco Secure Workload	Сетевой	OSI	2026-05-21	✓
19	Критическая	CVE-2024-9643	Four-Faith F3x36	Сетевой	ACE	2026-05-21	✗
20	Критическая	CVE-2024-9644	Four-Faith F3x36	Сетевой	OSI	2026-05-21	✗
21	Высокая	CVE-2026-45584	Microsoft Malware Protection Engine	Сетевой	ACE	2026-05-21	✓
22	Критическая	CVE-2026-9082	Drupal API	Сетевой	ACE	2026-05-21	✓
23	Высокая	CVE-2026-35554	Apache Kafka	Сетевой	PE	2026-05-21	✓
24	Высокая	CVE-2026-33155	DeepDiff	Сетевой	DoS	2026-05-21	✓
25	Высокая	CVE-2026-42001	PowerDNS Authoritative	Сетевой	DoS	2026-05-20	✓
26	Высокая	CVE-2026-33840	Windows 11 24H2	Локальный	PE	2026-05-13	✓
27	Высокая	CVE-2026-7377	Gitlab	Сетевой	XSS\CSS	2026-05-14	✓
28	Высокая	CVE-2026-40406	Windows 10 1607	Сетевой	OSI	2026-05-14	✓

29	Высокая	CVE-2026-40405	Windows 11 24H2	Сетевой	DoS	2026-05-14	✓
30	Высокая	CVE-2026-40419	Microsoft 365 Apps for Enterprise	Локальный	PE	2026-05-14	✓
31	Высокая	CVE-2026-40417	Microsoft Dynamics 365 Business Central 2024 Release Wave 2	Локальный	PE	2026-05-14	✓
32	Высокая	CVE-2026-34676	Adobe Substance 3D Painter	Локальный	ACE	2026-05-14	✓
33	Высокая	CVE-2026-34675	Adobe Substance 3D Painter	Локальный	ACE	2026-05-14	✓
34	Высокая	CVE-2026-41088	Windows 10 21H2	Локальный	PE	2026-05-14	✓
35	Высокая	CVE-2025-53844	FortiOS	Сетевой	ACE	2026-05-13	✓
36	Высокая	CVE-2026-34337	Windows 10 1809	Локальный	PE	2026-05-13	✓
37	Высокая	CVE-2026-32204	Azure Monitor Agent	Локальный	PE	2026-05-14	✓
38	Высокая	CVE-2026-33835	Windows 10 1809	Локальный	PE	2026-05-13	✓
39	Высокая	CVE-2026-35436	Microsoft 365 Apps for Enterprise	Локальный	PE	2026-05-13	✓
40	Высокая	CVE-2026-40418	Microsoft 365 Apps for Enterprise	Локальный	PE	2026-05-13	✓
41	Высокая	CVE-2026-34334	Windows 10 1607	Локальный	PE	2026-05-13	✓
42	Высокая	CVE-2026-34338	Windows 10 1607	Локальный	PE	2026-05-13	✓
43	Высокая	CVE-2026-42896	Windows 11 24H2	Локальный	PE	2026-05-14	✓

44	Высокая	CVE-2026-42899	.NET	Сетевой	DoS	2026-05-14	✓
45	Высокая	CVE-2026-40381	Azure Connected Machine Agent	Локальный	PE	2026-05-13	✓
46	Критическая	CVE-2026-40402	Windows 11 23H2	Локальный	PE	2026-05-13	✓
47	Критическая	CVE-2026-42823	Azure Logic Apps	Сетевой	PE	2026-05-13	✓
48	Высокая	CVE-2026-40377	Windows 10 1607	Локальный	PE	2026-05-14	✓
49	Высокая	CVE-2026-34636	Adobe Premiere Pro	Локальный	ACE	2026-05-13	✓
50	Критическая	CVE-2026-34660	Adobe Connect Desktop Application	Сетевой	PE	2026-05-14	✓
51	Высокая	CVE-2026-34640	Adobe Media Encoder	Локальный	ACE	2026-05-13	✓
52	Высокая	CVE-2026-34674	Adobe Substance 3D Sampler	Локальный	ACE	2026-05-14	✓
53	Высокая	CVE-2026-40367	Microsoft 365 Apps for Enterprise	Локальный	ACE	2026-05-13	✓
54	Высокая	CVE-2026-34638	Adobe Premiere Pro	Локальный	ACE	2026-05-13	✓
55	Высокая	CVE-2026-34639	Adobe Media Encoder	Локальный	ACE	2026-05-13	✓
56	Высокая	CVE-2026-34683	Adobe Substance 3D Designer	Локальный	ACE	2026-05-14	✓
57	Высокая	CVE-2026-34682	Adobe Substance 3D Designer	Локальный	ACE	2026-05-14	✓
58	Высокая	CVE-2026-34681	Adobe Substance 3D Designer	Локальный	ACE	2026-05-14	✓

59	Высокая	CVE-2026-34684	Adobe Substance 3D Designer	Локальный	ACE	2026-05-14	✓
60	Критическая	CVE-2026-34659	Adobe Connect Desktop Application	Сетевой	ACE	2026-05-14	✓
61	Высокая	CVE-2026-40370	Microsoft SQL Server 2025 (GDR)	Сетевой	ACE	2026-05-13	✓
62	Высокая	CVE-2026-41095	Windows Server 2012 R2	Локальный	PE	2026-05-14	✓
63	Высокая	CVE-2026-35421	Windows 10 1607	Локальный	ACE	2026-05-13	✓
64	Высокая	CVE-2026-41259	Mastodon	Сетевой	SB	2026-05-14	✓
65	Критическая	CVE-2026-34263	SAP Commerce Cloud	Сетевой	ACE	2026-05-14	✓
66	Критическая	CVE-2026-20182	Catalyst SD-WAN Manager	Сетевой	SB	2026-05-15	✓
67	Критическая	CVE-2026-21515	Azure IOT Central	Сетевой	PE	2026-05-06	✓
68	Высокая	CVE-2026-45585	Windows 11 24H2	Локальный	OSI	2026-05-14	✓
69	Высокая	BDU:2026-06826	Windows 11	Локальный	PE	2026-05-14	✓
70	Высокая	CVE-2026-26150	Microsoft Purview eDiscovery	Сетевой	PE	2026-05-06	✓
71	Критическая	CVE-2026-44277	FortiAuthenticator	Сетевой	ACE	2026-05-14	✓
72	Высокая	CVE-2026-34687	Illustrator 2025	Локальный	ACE	2026-05-14	✓
73	Высокая	CVE-2026-32172	Microsoft Power Apps	Сетевой	ACE	2026-05-06	✓

74	Высокая	CVE-2026-41105	Azure Monitor Action Group	Сетевой	PE	2026-05-12	✓
75	Критическая	CVE-2026-40379	Microsoft Enterprise Security Token Service	Сетевой	OSI	2026-05-12	✓
76	Критическая	CVE-2026-33823	Microsoft Teams	Сетевой	ACE	2026-05-12	✓
77	Критическая	CVE-2026-33844	Azure Managed Instance for Apache Cassandra	Сетевой	ACE	2026-05-12	✓
78	Высокая	CVE-2026-35435	Azure AI Foundry	Сетевой	PE	2026-05-12	✓
79	Критическая	CVE-2026-33102	Microsoft 365 Copilot	Сетевой	PE	2026-05-06	✓
80	Критическая	CVE-2026-32210	Microsoft Dynamics 365	Сетевой	ACE	2026-05-06	✓
81	Высокая	CVE-2026-34661	Illustrator 2025	Локальный	ACE	2026-05-14	✓
82	Высокая	CVE-2026-28377	Grafana Tempo	Сетевой	OSI	2026-03-24	✓
83	Критическая	CVE-2026-6771	Firefox	Сетевой	SB	2026-04-22	✓
84	Высокая	CVE-2026-6780	Firefox	Сетевой	DoS	2026-04-22	✓
85	Высокая	CVE-2026-6776	Firefox	Локальный	LoI	2026-04-22	✓
86	Высокая	CVE-2026-6785	Firefox	Сетевой	ACE	2026-04-22	✓
87	Высокая	CVE-2026-6786	Firefox	Сетевой	ACE	2026-04-22	✓
88	Высокая	CVE-2026-6772	Firefox	Сетевой	SB	2026-04-22	✓

89	Высокая	CVE-2026-6773	Firefox	Сетевой	DoS	2026-04-22	✓
90	Высокая	CVE-2026-6781	Firefox	Сетевой	DoS	2026-04-22	✓
91	Критическая	CVE-2026-35512	xrdp	Сетевой	ACE	2026-04-22	✓
92	Высокая	CVE-2026-6784	Firefox	Сетевой	ACE	2026-04-22	✓
93	Высокая	CVE-2026-32107	xrdp	Локальный	ACE	2026-04-22	✓
94	Высокая	CVE-2026-6073	Gitlab	Сетевой	ACE	2026-05-18	✓
95	Высокая	CVE-2026-7481	Gitlab	Сетевой	ACE	2026-05-18	✓
96	Высокая	CVE-2026-34637	Adobe Premiere Pro	Локальный	ACE	2026-05-13	✓
97	Высокая	CVE-2026-24880	Tomcat	Сетевой	SB	2026-05-15	✓
98	Критическая	CVE-2026-32623	xrdp	Сетевой	DoS	2026-04-22	✓
99	Высокая	CVE-2026-33689	xrdp	Сетевой	DoS	2026-04-22	✓
100	Критическая	CVE-2026-0265	PAN-OS	Сетевой	SB	2026-05-18	✓
101	Высокая	CVE-2026-20224	Catalyst SD-WAN Manager	Сетевой	SB	2026-05-18	✓
102	Высокая	CVE-2025-32372	DNN	Сетевой	CSRF	2026-05-18	✓
103	Критическая	CVE-2026-33516	xrdp	Сетевой	DoS	2026-04-22	✓

104	Высокая	CVE-2026-1322	Gitlab	Сетевой	OSI	2026-05-18	✓
105	Высокая	CVE-2026-1184	Gitlab	Сетевой	DoS	2026-05-18	✓
106	Высокая	CVE-2025-14870	Gitlab	Сетевой	DoS	2026-05-18	✓
107	Критическая	CVE-2026-25244	WebdriverIO	Сетевой	ACE	2026-05-20	✓
108	Высокая	CVE-2026-34632	Photoshop	Локальный	PE	2026-05-21	✓
109	Высокая	CVE-2026-35058	Ubuntu	Сетевой	DoS	2026-05-21	✓
110	Высокая	CVE-2026-41091	Microsoft Malware Protection Engine	Локальный	PE	2026-05-21	✓
111	Высокая	CVE-2026-29047	РЕД ОС	Сетевой	ACE	2026-05-20	✓
112	Критическая	CVE-2026-26263	РЕД ОС	Сетевой	ACE	2026-05-21	✓
113	Высокая	CVE-2026-41086	Windows Admin Center in Azure Portal	Сетевой	PE	2026-05-22	✓
114	Высокая	CVE-2026-45250	FreeBSD	Локальный	DoS	2026-05-21	✓
115	Высокая	CVE-2026-40415	Windows 10 1809	Сетевой	ACE	2026-05-22	✓
116	Высокая	CVE-2026-40399	Windows 10 1607	Локальный	PE	2026-05-22	✓
117	Высокая	CVE-2026-40397	Windows 10 1607	Локальный	PE	2026-05-22	✓
118	Высокая	BDU:2026-07126	PT Dephaze	Сетевой	ACE	2026-05-21	✓

119	Высокая	BDU:2026-07127	PT Dephaze	Сетевой	ACE	2026-05-21	✓
120	Высокая	CVE-2026-40408	Windows 10 1607	Локальный	PE	2026-05-22	✓
121	Критическая	CVE-2026-32633	РЕД ОС	Сетевой	OSI	2026-05-20	✓
122	Критическая	CVE-2026-32611	РЕД ОС	Сетевой	ACE	2026-05-20	✓
123	Высокая	CVE-2026-32610	РЕД ОС	Сетевой	OSI	2026-05-18	✓
124	Высокая	CVE-2026-32634	РЕД ОС	Смежная сеть	OSI	2026-05-22	✓

1

Краткое описание: Повышение привилегий в Joomla!

Идентификатор уязвимости: CVE-2026-48899

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Joomla!: 3.0.0 - 6.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка сертификатов.

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

Оценка CVSSv4: 5.0 AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://developer.joomla.org/security-centre/1043-20260511-core-mfa-authentication-bypass.html
- https://developer.joomla.org/security-centre/950-20260511-core-mfa-authentication-bypass.html
- https://developer.joomla.org/security-centre/1044-20260512-core-mfa-authentication-bypass.html
- https://developer.joomla.org/security-centre/1045-20260513-core-privilege-escalation-through-com-users-batch-task.html
- https://developer.joomla.org/security-centre/950-20260513-core-privilege-escalation-through-com-users-batch-task.html
- https://developer.joomla.org/security-centre/1046-20260514-core-privilege-escalation-through-com-users-webservice-endpoints.html
- https://developer.joomla.org/security-centre/950-20260514-core-privilege-escalation-through-com-users-webservice-endpoints.html
- https://developer.joomla.org/security-centre/1047-20260515-core-incorrect-access-control-in-sample-data-plugins.html
- https://developer.joomla.org/security-centre/1048-20260516-core-incorrect-access-control-in-com-scheduler.html
- https://developer.joomla.org/security-centre/950-20260516-core-incorrect-access-control-in-com-scheduler.html
- https://developer.joomla.org/security-centre/1049-20260517-core-incorrect-cache-key-construction-for-inputfilter-objects.html

- https://developer.joomla.org/security-centre/1050-20260518-core-transport-encryption-downgrade-for-password-and-username-reset-links.html
- https://developer.joomla.org/security-centre/1051-20260519-framework-inadequate-content-filtering-within-the-checkattribute-filter-code.html
- https://developer.joomla.org/security-centre/1052-20260520-framework-inadequate-content-filtering-within-the-cleanattributes-filter-code.html

2

Краткое описание: Повышение привилегий в Joomla!

Идентификатор уязвимости: CVE-2026-48904

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Joomla!: 3.0.0 - 6.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка входных 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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://developer.joomla.org/security-centre/1043-20260511-core-mfa-authentication-bypass.html
- https://developer.joomla.org/security-centre/950-20260511-core-mfa-authentication-bypass.html
- https://developer.joomla.org/security-centre/1044-20260512-core-mfa-authentication-bypass.html
- https://developer.joomla.org/security-centre/1045-20260513-core-privilege-escalation-through-com-users-batch-task.html
- https://developer.joomla.org/security-centre/950-20260513-core-privilege-escalation-through-com-users-batch-task.html
- https://developer.joomla.org/security-centre/1046-20260514-core-privilege-escalation-through-com-users-webservice-endpoints.html
- https://developer.joomla.org/security-centre/950-20260514-core-privilege-escalation-through-com-users-webservice-endpoints.html
- https://developer.joomla.org/security-centre/1047-20260515-core-incorrect-access-control-in-sample-data-plugins.html
- https://developer.joomla.org/security-centre/1048-20260516-core-incorrect-access-control-in-com-scheduler.html
- https://developer.joomla.org/security-centre/950-20260516-core-incorrect-access-control-in-com-scheduler.html
- https://developer.joomla.org/security-centre/1049-20260517-core-incorrect-cache-key-construction-for-inputfilter-objects.html

- https://developer.joomla.org/security-centre/1050-20260518-core-transport-encryption-downgrade-for-password-and-username-reset-links.html
- https://developer.joomla.org/security-centre/1051-20260519-framework-inadequate-content-filtering-within-the-checkattribute-filter-code.html
- https://developer.joomla.org/security-centre/1052-20260520-framework-inadequate-content-filtering-within-the-cleanattributes-filter-code.html

3

Краткое описание: Повышение привилегий в Joomla!

Идентификатор уязвимости: CVE-2026-48898

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Joomla!: 3.0.0 - 6.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка входных 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: 9.8 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://developer.joomla.org/security-centre/1043-20260511-core-mfa-authentication-bypass.html
- https://developer.joomla.org/security-centre/950-20260511-core-mfa-authentication-bypass.html
- https://developer.joomla.org/security-centre/1044-20260512-core-mfa-authentication-bypass.html
- https://developer.joomla.org/security-centre/1045-20260513-core-privilege-escalation-through-com-users-batch-task.html
- https://developer.joomla.org/security-centre/950-20260513-core-privilege-escalation-through-com-users-batch-task.html
- https://developer.joomla.org/security-centre/1046-20260514-core-privilege-escalation-through-com-users-webservice-endpoints.html
- https://developer.joomla.org/security-centre/950-20260514-core-privilege-escalation-through-com-users-webservice-endpoints.html
- https://developer.joomla.org/security-centre/1047-20260515-core-incorrect-access-control-in-sample-data-plugins.html
- https://developer.joomla.org/security-centre/1048-20260516-core-incorrect-access-control-in-com-scheduler.html
- https://developer.joomla.org/security-centre/950-20260516-core-incorrect-access-control-in-com-scheduler.html
- https://developer.joomla.org/security-centre/1049-20260517-core-incorrect-cache-key-construction-for-inputfilter-objects.html

- https://developer.joomla.org/security-centre/1050-20260518-core-transport-encryption-downgrade-for-password-and-username-reset-links.html
- https://developer.joomla.org/security-centre/1051-20260519-framework-inadequate-content-filtering-within-the-checkattribute-filter-code.html
- https://developer.joomla.org/security-centre/1052-20260520-framework-inadequate-content-filtering-within-the-cleanattributes-filter-code.html

4

Краткое описание: Получение конфиденциальной информации в Apache CXF

Идентификатор уязвимости: CVE-2026-44930
BDU:2026-07399

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

Уязвимый продукт: Apache CXF: 3.0.0 - 4.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Некорректная проверка сертификатов.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://lists.apache.org/api/email.lua?id=nr1l8k9kgq4rx61ytfkq0bt8w549o1rv
- https://lists.apache.org/api/email.lua?id=1xbchhjzsd17ypfk2mxyr2kwb3w2ml93
- https://cxf.apache.org/
- https://lists.apache.org/api/email.lua?id=jop2sf8d8hvbcy93jjgyh8cx91vggshf
- https://bdu.fstec.ru/vul/2026-07399

5

Краткое описание: Выполнение произвольного кода в Apache CXF

Идентификатор уязвимости: CVE-2026-44417

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Apache CXF: 3.0.0 - 4.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://lists.apache.org/api/email.lua?id=nr1l8k9kgq4rx61ytfkq0bt8w549o1rv
- https://lists.apache.org/api/email.lua?id=1xbchhjzsd17ypfk2mxyr2kwb3w2ml93
- https://cxf.apache.org/
- https://lists.apache.org/api/email.lua?id=jop2sf8d8hvbcy93jjgyh8cx91vggshf

6

Краткое описание: Выполнение произвольного кода в Codehaus plexus-utils

Идентификатор уязвимости: CVE-2025-67030

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

Уязвимый продукт: Codehaus plexus-utils: 3.0 - 4.0.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://github.com/codehaus-plexus/plexus-utils/commit/6d780b3378829318ba5c2d29547e0012d5b29642
- https://github.com/codehaus-plexus/plexus-utils/issues/294
- https://bugzilla.redhat.com/show_bug.cgi?id=2451409

7

Краткое описание: Отказ в обслуживании в LibTIFF

Идентификатор уязвимости: CVE-2026-4775

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

Уязвимый продукт: LibTIFF: 4.7.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Запись за пределами буфера.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.8 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: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://gitlab.com/libtiff/libtiff/-/work_items/787
- https://gitlab.com/libtiff/libtiff/-/commit/782a11d6b5b61c6dc21e714950a4af5bf89f023c

8

Краткое описание: Получение конфиденциальной информации в Date iCal module for Drupal

Идентификатор уязвимости: CVE-2026-8495

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Date iCal: до 4.0.15

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2026-05-26 / 2026-05-26

Ссылки на источник:

- https://www.drupal.org/sa-contrib-2026-037

9

Краткое описание: Получение конфиденциальной информации в LiteSpeed User-End cPanel Plugin

Идентификатор уязвимости: CVE-2026-48172

Идентификатор программной ошибки: CWE-266 Некорректное назначение привилегий

Уязвимый продукт: LiteSpeed User-End cPanel Plugin: до 2.4.7
LiteSpeed WHM Plugin: до 5.3.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 10.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-25 / 2026-05-26

Ссылки на источник:

- https://blog.litespeedtech.com/2026/05/21/security-update-for-litespeed-cpanel-plugin/
- https://support.cpanel.net/hc/en-us/articles/40599423437079-Security-LiteSpeed-plugin-automatically-removed-during-nightly-update-May-19-2026

10

Краткое описание: Выполнение произвольного кода в NGINX ngx_http_rewrite_module module

Идентификатор уязвимости: CVE-2026-9256
BDU:2026-07182

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

Уязвимый продукт: NGINX Plus: R28 - 37.0.0
NGINX Open Source: 0.1.17 - 1.30.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 9.0 AV:N/AC:H/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-25 / 2026-05-25

Ссылки на источник:

- https://my.f5.com/manage/s/article/K000161377
- https://bdu.fstec.ru/vul/2026-07182

11

Краткое описание: Выполнение произвольного кода в Docker Desktop

Идентификатор уязвимости: CVE-2026-5843

Идентификатор программной ошибки: CWE-829 Использование функций недоверенных источников

Уязвимый продукт: Docker Desktop: 4.0.0 - 4.70.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-22 / 2026-05-22

Ссылки на источник:

- https://docs.docker.com/security/security-announcements/#docker-desktop-4710-security-update-cve-2026-5843
- https://docs.docker.com/desktop/release-notes/#4710

12

Краткое описание: Выполнение произвольного кода в Docker Desktop

Идентификатор уязвимости: CVE-2026-5817

Идентификатор программной ошибки: CWE-829 Использование функций недоверенных источников

Уязвимый продукт: Docker Desktop: 4.0.0 - 4.67.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-22 / 2026-05-22

Ссылки на источник:

- https://docs.docker.com/security/security-announcements/#docker-desktop-4680-security-update-cve-2026-5817
- https://docs.docker.com/desktop/release-notes/#4680

13

Краткое описание: Получение конфиденциальной информации в Kata Containers

Идентификатор уязвимости: CVE-2026-41326

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

Уязвимый продукт: Kata Containers: 1.9.4 - 3.28.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-22 / 2026-05-22

Ссылки на источник:

- https://github.com/kata-containers/kata-containers/security/advisories/GHSA-989w-4xr2-ww9m
- https://github.com/kata-containers/kata-containers/blob/c980b6e191e174053681fb30817736e040554c10/src/agent/src/main.rs#L460-L474
- https://github.com/kata-containers/kata-containers/security/advisories/GHSA-q49m-57vm-c8cc
- https://github.com/kata-containers/kata-containers/security/advisories

Краткое описание: Отказ в обслуживании в ISC BIND

Идентификатор уязвимости: CVE-2026-3039

Идентификатор программной ошибки: CWE-771 Отсутствие ссылки на активный выделенный ресурс

Уязвимый продукт: ISC BIND: до 9.18.49, 9.18.49-S1, 9.20.23, 9.20.23-S1, 9.21.22

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

14

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: 2026-05-22 / 2026-05-22

Ссылки на источник:

- https://kb.isc.org/docs/cve-2026-5950
- https://kb.isc.org/docs/cve-2026-5947
- https://kb.isc.org/docs/cve-2026-5946
- https://kb.isc.org/docs/cve-2026-3593
- https://kb.isc.org/docs/cve-2026-3592
- https://kb.isc.org/docs/cve-2026-3039

Краткое описание: Отказ в обслуживании в ISC BIND

Идентификатор уязвимости: CVE-2026-5946

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: ISC BIND: до 9.18.49, 9.18.49-S1, 9.20.23, 9.20.23-S1, 9.21.22

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных DNS-запросов.

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.

15 **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: 2026-05-22 / 2026-05-22

Ссылки на источник:

- https://kb.isc.org/docs/cve-2026-5950
- https://kb.isc.org/docs/cve-2026-5947
- https://kb.isc.org/docs/cve-2026-5946
- https://kb.isc.org/docs/cve-2026-3593
- https://kb.isc.org/docs/cve-2026-3592
- https://kb.isc.org/docs/cve-2026-3039

16

Краткое описание: Отказ в обслуживании в ISC BIND

Идентификатор уязвимости: CVE-2026-5947

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

Уязвимый продукт: ISC BIND: до 9.18.49, 9.18.49-S1, 9.20.23, 9.20.23-S1, 9.21.22

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Использование памяти после ее освобождения.

Последствия эксплуатации: Отказ в обслуживании

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

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: 2026-05-22 / 2026-05-22

Ссылки на источник:

- https://kb.isc.org/docs/cve-2026-5950
- https://kb.isc.org/docs/cve-2026-5947
- https://kb.isc.org/docs/cve-2026-5946
- https://kb.isc.org/docs/cve-2026-3593
- https://kb.isc.org/docs/cve-2026-3592
- https://kb.isc.org/docs/cve-2026-3039

17

Краткое описание: Выполнение произвольного кода в ConnectWise Automate

Идентификатор уязвимости: CVE-2026-9089

Идентификатор программной ошибки: CWE-494 Загрузка кода без проверки его целостности

Уязвимый продукт: Automate: до 2026.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://www.connectwise.com/company/trust/security-bulletins/2026-05-21-connectwise-automate-bulletin
- https://www.first.org/cvss/calculator/3-1#CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

18

Краткое описание: Получение конфиденциальной информации в Cisco Secure Workload

Идентификатор уязвимости: CVE-2026-20223

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

Уязвимый продукт: Cisco Secure Workload: до 3.10.8.3, 4.0.3.17

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-csw-pnbsa-g8WEnuy
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwt99942

19

Краткое описание: Выполнение произвольного кода в Four-Faith F3x36

Идентификатор уязвимости: CVE-2024-9643

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

Уязвимый продукт: F3x36: 2.0

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Использование жестко закодированных учетных данных

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://vulncheck.com/advisories/four-faith-hidden-api
- https://vulncheck.com/advisories/four-faith-hard-coded-creds

20

Краткое описание: Получение конфиденциальной информации в Four-Faith F3x36

Идентификатор уязвимости: CVE-2024-9644

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

Уязвимый продукт: F3x36: 2.0

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://vulncheck.com/advisories/four-faith-hidden-api
- https://vulncheck.com/advisories/four-faith-hard-coded-creds

21

Краткое описание: Выполнение произвольного кода в Microsoft Malware Protection Engine

Идентификатор уязвимости: CVE-2026-45584

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

Уязвимый продукт: Microsoft Malware Protection Engine: до 1.1.26040.8

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45584

22

Краткое описание: Выполнение произвольного кода в Drupal API

Идентификатор уязвимости: CVE-2026-9082

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

Уязвимый продукт: Drupal: 8.9.0 beta1 - 11.3.9

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-05-21 / 2026-05-22

Ссылки на источник:

- https://www.drupal.org/sa-core-2026-004

23

Краткое описание: Повышение привилегий в Apache Kafka

Идентификатор уязвимости: CVE-2026-35554

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

Уязвимый продукт: Apache Kafka: до 3.9.2, 4.0.2, 4.1.2, 4.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Использование памяти после ее освобождения.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 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: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://issues.apache.org/jira/browse/KAFKA-19012
- https://lists.apache.org/thread/f07x7j8ovyqhjd1to25jsnqbm6wj01d6
- http://www.openwall.com/lists/oss-security/2026/04/07/6

24

Краткое описание: Отказ в обслуживании в DeepDiff

Идентификатор уязвимости: CVE-2026-33155

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

Уязвимый продукт: deepdiff: 5.0.0 - 8.6.1

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://github.com/qlustered/deepdiff/commit/0d07ec21d12b46ef4e489383b363eadc22d990fb
- https://github.com/qlustered/deepdiff/security/advisories/GHSA-54jj-px8x-5w5q

25

Краткое описание: Отказ в обслуживании в PowerDNS Authoritative

Идентификатор уязвимости: CVE-2026-42001

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

Уязвимый продукт: PowerDNS Authoritative: 2.9.21.1 - 5.0.4

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://docs.powerdns.com/authoritative/security-advisories/powerdns-advisory-2026-06.html

26

Краткое описание: Повышение привилегий в Windows 11 24H2

Идентификатор уязвимости: CVE-2026-33840
BDU:2026-06740

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 11 24H2: до 10.0.26100.8390
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33840
- https://bdu.fstec.ru/vul/2026-06740

27

Краткое описание: Межсайтовый скриптинг в Gitlab

Идентификатор уязвимости: CVE-2026-7377
BDU:2026-06813

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

Уязвимый продукт: Gitlab: от 18.11 до 18.11.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Межсайтовый скриптинг

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

Оценка CVSSv3: 8.7 AV:N/AC:L/PR:L/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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://darkeye.org/vuln/cve/CVE-2026-7377
- https://docs.gitlab.com/releases/patches/patch-release-gitlab-18-11-3-released/
- https://github.com/advisories/GHSA-cv3h-4g8c-4vw6
- https://www.thehackerwire.com/gitlab-ee-authenticated-xss-in-analytics-dashboards/
- https://bdu.fstec.ru/vul/2026-06813

28

Краткое описание: Получение конфиденциальной информации в Windows 10 1607

Идентификатор уязвимости: CVE-2026-40406
BDU:2026-06803

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40406
- https://bdu.fstec.ru/vul/2026-06803

29

Краткое описание: Отказ в обслуживании в Windows 11 24H2

Идентификатор уязвимости: CVE-2026-40405
BDU:2026-06801

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Windows 11 24H2: до 10.0.26100.8390
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

Категория уязвимого продукта: Операционные системы Microsoft 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: 7.5 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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40405
- https://bdu.fstec.ru/vul/2026-06801

30

Краткое описание: Повышение привилегий в Microsoft 365 Apps for Enterprise

Идентификатор уязвимости: CVE-2026-40419
BDU:2026-06800

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: -
Microsoft Office LTSC 2024: -
Microsoft Office 2019: -

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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40419
- https://bdu.fstec.ru/vul/2026-06800

31

Краткое описание: Повышение привилегий в Microsoft Dynamics 365 Business Central 2024 Release Wave 2

Идентификатор уязвимости: CVE-2026-40417
BDU:2026-06798

Идентификатор программной ошибки: CWE-1038 Небезопасная автоматическая оптимизация

Уязвимый продукт: Microsoft Dynamics 365 Business Central 2024 Release Wave 2: до 25.18
Microsoft Dynamics 365 Business Central Release Wave 2 2025: до 27.6
Microsoft Dynamics 365 Business Central Release Wave 1 2025: до 26.12
Microsoft Dynamics 365 Business Central 2026 Release Wave 1: до 28.1

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40417
- https://bdu.fstec.ru/vul/2026-06798

32

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

Идентификатор уязвимости: CVE-2026-34676
BDU:2026-06797

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Painter: до 12.0.2 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Запись за пределами буфера.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_painter/apsb26-55.html
- https://bdu.fstec.ru/vul/2026-06797

33

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

Идентификатор уязвимости: CVE-2026-34675
BDU:2026-06796

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Painter: до 12.0.2 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Запись за пределами буфера.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_painter/apsb26-55.html
- https://bdu.fstec.ru/vul/2026-06796

34

Краткое описание: Повышение привилегий в Windows 10 21H2

Идентификатор уязвимости: CVE-2026-41088
BDU:2026-06786

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

Уязвимый продукт: Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

Категория уязвимого продукта: Операционные системы Microsoft 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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41088

- https://bdu.fstec.ru/vul/2026-06786

35

Краткое описание: Выполнение произвольного кода в FortiOS

Идентификатор уязвимости: CVE-2025-53844
BDU:2026-06783

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: FortiOS: от 7.2.0 до 7.2.12

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://fortiguard.fortinet.com/psirt/FG-IR-26-123
- https://bdu.fstec.ru/vul/2026-06783

36

Краткое описание: Повышение привилегий в Windows 10 1809

Идентификатор уязвимости: CVE-2026-34337
BDU:2026-06781

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-34337
- https://bdu.fstec.ru/vul/2026-06781

37

Краткое описание: Повышение привилегий в Azure Monitor Agent

Идентификатор уязвимости: CVE-2026-32204
BDU:2026-06748

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

Уязвимый продукт: Azure Monitor Agent: до 1.14.0

Категория уязвимого продукта: Операционные системы Microsoft 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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32204
- https://bdu.fstec.ru/vul/2026-06748

38

Краткое описание: Повышение привилегий в Windows 10 1809

Идентификатор уязвимости: CVE-2026-33835
BDU:2026-06769

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33835
- https://bdu.fstec.ru/vul/2026-06769

39

Краткое описание: Повышение привилегий в Microsoft 365 Apps for Enterprise

Идентификатор уязвимости: CVE-2026-35436
BDU:2026-06751

Идентификатор программной ошибки: CWE-1052 Чрезмерное использование жестко закодированных литералов для инициализации

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: -
Microsoft Office LTSC 2024: -
Microsoft Office 2019: -

Категория уязвимого продукта: Операционные системы Microsoft и их 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: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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35436
- https://feedly.com/cve/CVE-2026-35436
- https://bdu.fstec.ru/vul/2026-06751

Краткое описание: Повышение привилегий в Microsoft 365 Apps for Enterprise

Идентификатор уязвимости: CVE-2026-40418
BDU:2026-06754

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft Office LTSC 2021: -
Microsoft Office LTSC 2024: -
Microsoft Office 2019: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

40 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40418
- https://feedly.com/cve/CVE-2026-40418
- https://bdu.fstec.ru/vul/2026-06754

41

Краткое описание: Повышение привилегий в Windows 10 1607

Идентификатор уязвимости: CVE-2026-34334
BDU:2026-06755

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

Категория уязвимого продукта: Операционные системы Microsoft 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: 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-34334
- https://bdu.fstec.ru/vul/2026-06755

42

Краткое описание: Повышение привилегий в Windows 10 1607

Идентификатор уязвимости: CVE-2026-34338
BDU:2026-06771

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-34338
- https://bdu.fstec.ru/vul/2026-06771

43

Краткое описание: Повышение привилегий в Windows 11 24H2

Идентификатор уязвимости: CVE-2026-42896
BDU:2026-06762

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

Уязвимый продукт: Windows 11 24H2: до 10.0.26100.8390
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42896
- https://feedly.com/cve/CVE-2026-42896
- https://bdu.fstec.ru/vul/2026-06762

44

Краткое описание: Отказ в обслуживании в .NET

Идентификатор уязвимости: CVE-2026-42899
BDU:2026-06767

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

Уязвимый продукт: .NET: от 9.0 до 9.0.16

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42899
- https://feedly.com/cve/CVE-2026-42899
- https://bdu.fstec.ru/vul/2026-06767

45

Краткое описание: Повышение привилегий в Azure Connected Machine Agent

Идентификатор уязвимости: CVE-2026-40381
BDU:2026-06857

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Azure Connected Machine Agent: до 1.63

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40381
- https://bdu.fstec.ru/vul/2026-06857

Краткое описание: Повышение привилегий в Windows 11 23H2

Идентификатор уязвимости: CVE-2026-40402
BDU:2026-06858

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 11 23H2: до 10.0.22631.7079
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022 (Server Core installation): до 10.0.20348.5074

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40402
- https://bdu.fstec.ru/vul/2026-06858

47

Краткое описание: Повышение привилегий в Azure Logic Apps

Идентификатор уязвимости: CVE-2026-42823
BDU:2026-06866

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Azure Logic Apps: -

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42823
- https://bdu.fstec.ru/vul/2026-06866

48

Краткое описание: Повышение привилегий в Windows 10 1607

Идентификатор уязвимости: CVE-2026-40377
BDU:2026-06871

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40377
- https://bdu.fstec.ru/vul/2026-06871

49

Краткое описание: Выполнение произвольного кода в Adobe Premiere Pro

Идентификатор уязвимости: CVE-2026-34636
BDU:2026-06882

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Premiere Pro: до 25.6.4 включительно
Adobe Premiere: до 26.0.2 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Запись за пределами буфера.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://helpx.adobe.com/security/products/premiere_pro/apsb26-46.html
- https://bdu.fstec.ru/vul/2026-06882

50

Краткое описание: Повышение привилегий в Adobe Connect Desktop Application

Идентификатор уязвимости: CVE-2026-34660
BDU:2026-06877

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: Adobe Connect Desktop Application: до 2026.01.39

Категория уязвимого продукта: Прикладное программное обеспечение

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: 9.3 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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/connect/apsb26-50.html
- https://bdu.fstec.ru/vul/2026-06877

51

Краткое описание: Выполнение произвольного кода в Adobe Media Encoder

Идентификатор уязвимости: CVE-2026-34640
BDU:2026-06880

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

Уязвимый продукт: Adobe Media Encoder: до 26.0.2 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://helpx.adobe.com/security/products/media-encoder/apsb26-47.html
- https://bdu.fstec.ru/vul/2026-06880

52

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

Идентификатор уязвимости: CVE-2026-34674
BDU:2026-06881

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

Уязвимый продукт: Adobe Substance 3D Sampler: до 5.1.3 включительно

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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d-sampler/apsb26-54.html
- https://bdu.fstec.ru/vul/2026-06881

53

Краткое описание: Выполнение произвольного кода в Microsoft 365 Apps for Enterprise

Идентификатор уязвимости: CVE-2026-40367
BDU:2026-06856

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Microsoft 365 Apps for Enterprise: -
Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20280
Microsoft Office LTSC 2021: до 16.109.26051019
Microsoft Office LTSC 2024: до 16.109.26051019
Microsoft Office 2019: -
Microsoft Word 2016: до 16.0.5552.1000
Microsoft SharePoint Enterprise Server 2016: до 16.0.5552.1002
Microsoft SharePoint Server 2019: до 16.0.10417.20128

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.4 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40367
- https://bdu.fstec.ru/vul/2026-06856

54

Краткое описание: Выполнение произвольного кода в Adobe Premiere Pro

Идентификатор уязвимости: CVE-2026-34638
BDU:2026-06883

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Premiere Pro: до 25.6.4 включительно
Adobe Premiere: до 26.0.2 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://helpx.adobe.com/security/products/premiere_pro/apsb26-46.html
- https://bdu.fstec.ru/vul/2026-06883

55

Краткое описание: Выполнение произвольного кода в Adobe Media Encoder

Идентификатор уязвимости: CVE-2026-34639
BDU:2026-06884

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Media Encoder: до 26.0.2 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://helpx.adobe.com/security/products/media-encoder/apsb26-47.html
- https://bdu.fstec.ru/vul/2026-06884

56

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

Идентификатор уязвимости: CVE-2026-34683
BDU:2026-06900

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Designer: до 15.1.0 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_designer/apsb26-52.html
- https://bdu.fstec.ru/vul/2026-06900

57

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

Идентификатор уязвимости: CVE-2026-34682
BDU:2026-06901

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Designer: до 15.1.0 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_designer/apsb26-52.html
- https://bdu.fstec.ru/vul/2026-06901

58

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

Идентификатор уязвимости: CVE-2026-34681
BDU:2026-06902

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Designer: до 15.1.0 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_designer/apsb26-52.html
- https://bdu.fstec.ru/vul/2026-06902

59

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

Идентификатор уязвимости: CVE-2026-34684
BDU:2026-06903

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Designer: до 15.1.0 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_designer/apsb26-52.html
- https://bdu.fstec.ru/vul/2026-06903

60

Краткое описание: Выполнение произвольного кода в Adobe Connect Desktop Application

Идентификатор уязвимости: CVE-2026-34659
BDU:2026-06876

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Adobe Connect Desktop Application: до 2026.01.39

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/connect/apsb26-50.html
- https://bdu.fstec.ru/vul/2026-06876

61

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server 2025 (GDR)

Идентификатор уязвимости: CVE-2026-40370
BDU:2026-06855

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

Уязвимый продукт: Microsoft SQL Server 2025 (GDR): до 17.0.1115.1
Microsoft SQL Server 2022 (GDR): до 16.0.1180.1
Microsoft SQL Server 2019 (CU 32): до 15.0.4470.1
Microsoft SQL Server 2016 Service Pack 3 Azure Connect Feature Pack: до 13.0.7085.1
Microsoft SQL Server 2017 (CU 31): до 14.0.3530.2
Microsoft SQL Server 2016 Service Pack 3 (GDR): до 13.0.6490.1
Microsoft SQL Server 2019 (GDR): до 15.0.2170.1
Microsoft SQL Server 2017 (GDR): до 14.0.2110.2
Microsoft SQL Server 2022 (CU 24): до 16.0.4252.3
Microsoft SQL Server 2025 (CU4): до 17.0.4040.1

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40370
- https://bdu.fstec.ru/vul/2026-06855

62

Краткое описание: Повышение привилегий в Windows Server 2012 R2

Идентификатор уязвимости: CVE-2026-41095
BDU:2026-06875

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772

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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41095

- https://bdu.fstec.ru/vul/2026-06875

63

Краткое описание: Выполнение произвольного кода в Windows 10 1607

Идентификатор уязвимости: CVE-2026-35421
BDU:2026-06854

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

Категория уязвимого продукта: Операционные системы Microsoft 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: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: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35421
- https://bdu.fstec.ru/vul/2026-06854

64

Краткое описание: Обход безопасности в Mastodon

Идентификатор уязвимости: CVE-2026-41259
BDU:2026-06821

Идентификатор программной ошибки: CWE-841 Некорректный контроль за последовательностью выполняемых действий

Уязвимый продукт: Mastodon: до 4.3.22

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 7.5 AV:N/AC: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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://github.com/mastodon/mastodon/security/advisories/GHSA-5r37-qpwq-2jhh
- https://github.com/mastodon/mastodon/releases/tag/v4.5.9
- https://github.com/mastodon/mastodon/releases/tag/v4.4.16
- https://github.com/mastodon/mastodon/releases/tag/v4.3.22
- https://bdu.fstec.ru/vul/2026-06821

65

Краткое описание: Выполнение произвольного кода в SAP Commerce Cloud

Идентификатор уязвимости: CVE-2026-34263
BDU:2026-06822

Идентификатор программной ошибки: CWE-459 Неполная очистка

Уязвимый продукт: SAP Commerce Cloud: 2211-JDK21

Категория уязвимого продукта: Не определено

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://me.sap.com/notes/3733064
- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2026.html
- https://www.decryptiondigest.com/blog/sap-cve-2026-34263-commerce-cloud-rce-s4hana-sqli
- https://bdu.fstec.ru/vul/2026-06822

66

Краткое описание: Обход безопасности в Catalyst SD-WAN Manager

Идентификатор уязвимости: CVE-2026-20182
BDU:2026-06823

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Catalyst SD-WAN Manager: от 26.1 до 26.1.1.1
Cisco Catalyst SD-WAN Controller: от 26.1 до 26.1.1.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

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: 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: 2026-05-15 / 2026-05-15

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-06823

67

Краткое описание: Повышение привилегий в Azure IOT Central

Идентификатор уязвимости: CVE-2026-21515
BDU:2026-06824

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

Уязвимый продукт: Azure IOT Central: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Несанкционированный сбор информации.

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-21515
- https://bdu.fstec.ru/vul/2026-06824

68

Краткое описание: Получение конфиденциальной информации в Windows 11 24H2

Идентификатор уязвимости: CVE-2026-45585
BDU:2026-06825

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Windows 11 24H2: -
Windows Server 2025: -
Windows Server 2025 (Server Core installation): -
Windows 11 25H2: -
Windows 11 26H1: -

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 7.8 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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://github.com/Nightmare-Eclipse/YellowKey
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-45585
- https://bdu.fstec.ru/vul/2026-06825

69

Краткое описание: Повышение привилегий в Windows 11

Идентификатор уязвимости: BDU:2026-06826

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Windows 11: -
Windows Server 2022: -
Windows Server 2025: -

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://github.com/Nightmare-Eclipse/GreenPlasma
- https://bdu.fstec.ru/vul/2026-06826

70

Краткое описание: Повышение привилегий в Microsoft Purview eDiscovery

Идентификатор уязвимости: CVE-2026-26150
BDU:2026-06828

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

Уязвимый продукт: Microsoft Purview eDiscovery: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 8.6 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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-26150
- https://bdu.fstec.ru/vul/2026-06828

71

Краткое описание: Выполнение произвольного кода в FortiAuthenticator

Идентификатор уязвимости: CVE-2026-44277
BDU:2026-06829

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: FortiAuthenticator: от 6.5.0 до 6.5.7

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://fortiguard.fortinet.com/psirt/FG-IR-26-128
- https://github.com/0xBlackash/CVE-2026-44277
- https://bdu.fstec.ru/vul/2026-06829

72

Краткое описание: Выполнение произвольного кода в Illustrator 2025

Идентификатор уязвимости: CVE-2026-34687
BDU:2026-06833

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

Уязвимый продукт: Illustrator 2025: до 29.8.7
Illustrator 2026: до 30.4

Категория уязвимого продукта: Операционные системы Microsoft 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: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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/illustrator/apsb26-51.html
- https://bdu.fstec.ru/vul/2026-06833

73

Краткое описание: Выполнение произвольного кода в Microsoft Power Apps

Идентификатор уязвимости: CVE-2026-32172
BDU:2026-06830

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: Microsoft Power Apps: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.0 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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32172
- https://bdu.fstec.ru/vul/2026-06830

74

Краткое описание: Повышение привилегий в Azure Monitor Action Group

Идентификатор уязвимости: CVE-2026-41105
BDU:2026-06846

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

Уязвимый продукт: Azure Monitor Action Group: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 8.1 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: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41105
- https://bdu.fstec.ru/vul/2026-06846

75

Краткое описание: Получение конфиденциальной информации в Microsoft Enterprise Security Token Service

Идентификатор уязвимости: CVE-2026-40379
BDU:2026-06843

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

Уязвимый продукт: Microsoft Enterprise Security Token Service: -

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 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: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2026-40379
- https://vuldb.com/vuln/362021
- https://bdu.fstec.ru/vul/2026-06843

76

Краткое описание: Выполнение произвольного кода в Microsoft Teams

Идентификатор уязвимости: CVE-2026-33823
BDU:2026-06841

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Microsoft Teams: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.6 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: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33823
- https://bdu.fstec.ru/vul/2026-06841

77

Краткое описание: Выполнение произвольного кода в Azure Managed Instance for Apache Cassandra

Идентификатор уязвимости: CVE-2026-33844
BDU:2026-06844

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Azure Managed Instance for Apache Cassandra: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33844
- https://bdu.fstec.ru/vul/2026-06844

78

Краткое описание: Повышение привилегий в Azure AI Foundry

Идентификатор уязвимости: CVE-2026-35435
BDU:2026-06840

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Azure AI Foundry: -

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 8.6 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: 2026-05-12 / 2026-05-12

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-35435
- https://bdu.fstec.ru/vul/2026-06840

79

Краткое описание: Повышение привилегий в Microsoft 365 Copilot

Идентификатор уязвимости: CVE-2026-33102
BDU:2026-06837

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

Уязвимый продукт: Microsoft 365 Copilot: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-33102
- https://bdu.fstec.ru/vul/2026-06837

80

Краткое описание: Выполнение произвольного кода в Microsoft Dynamics 365

Идентификатор уязвимости: CVE-2026-32210
BDU:2026-06836

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

Уязвимый продукт: Microsoft Dynamics 365: -

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.3 AV: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: 2026-05-06 / 2026-05-06

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-32210
- https://bdu.fstec.ru/vul/2026-06836

81

Краткое описание: Выполнение произвольного кода в Illustrator 2025

Идентификатор уязвимости: CVE-2026-34661
BDU:2026-06835

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Illustrator 2025: до 29.8.7
Illustrator 2026: до 30.4

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: 2026-05-14 / 2026-05-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/illustrator/apsb26-51.html
- https://bdu.fstec.ru/vul/2026-06835

82

Краткое описание: Получение конфиденциальной информации в Grafana Tempo

Идентификатор уязвимости: CVE-2026-28377
BDU:2026-06943

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

Уязвимый продукт: Grafana Tempo: до 2.10.3

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-03-24 / 2026-03-24

Ссылки на источник:

- https://grafana.com/security/security-advisories/cve-2026-28377/
- https://bdu.fstec.ru/vul/2026-06943

83

Краткое описание: Обход безопасности в Firefox

Идентификатор уязвимости: CVE-2026-6771
BDU:2026-06947

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

Уязвимый продукт: Firefox: до 150
Firefox ESR: до 140.10
Thunderbird: до 150

Категория уязвимого продукта: Прикладное программное обеспечение

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://www.mozilla.org/security/advisories/mfsa2026-30/
- https://www.mozilla.org/security/advisories/mfsa2026-32/
- https://www.mozilla.org/security/advisories/mfsa2026-33/
- https://www.mozilla.org/security/advisories/mfsa2026-34/
- https://bdu.fstec.ru/vul/2026-06947

84

Краткое описание: Отказ в обслуживании в Firefox

Идентификатор уязвимости: CVE-2026-6780
BDU:2026-06949

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

Уязвимый продукт: Firefox: до 150
Thunderbird: до 150

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://www.mozilla.org/security/advisories/mfsa2026-30/
- https://www.mozilla.org/security/advisories/mfsa2026-33/
- https://bdu.fstec.ru/vul/2026-06949

85

Краткое описание: Потеря целостности в Firefox

Идентификатор уязвимости: CVE-2026-6776
BDU:2026-06950

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

Уязвимый продукт: Firefox: до 150
Firefox ESR: до 140.10
Thunderbird: до 150

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://www.mozilla.org/security/advisories/mfsa2026-30/
- https://www.mozilla.org/security/advisories/mfsa2026-32/
- https://www.mozilla.org/security/advisories/mfsa2026-33/
- https://www.mozilla.org/security/advisories/mfsa2026-34/
- https://bdu.fstec.ru/vul/2026-06950

86

Краткое описание: Выполнение произвольного кода в Firefox

Идентификатор уязвимости: CVE-2026-6785
BDU:2026-06953

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Firefox: до 150
Firefox ESR: до 115.35
Thunderbird: до 150
Thunderbird ESR: до 140.10

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: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://www.mozilla.org/security/advisories/mfsa2026-30/
- https://www.mozilla.org/security/advisories/mfsa2026-31/
- https://www.mozilla.org/security/advisories/mfsa2026-32/
- https://www.mozilla.org/security/advisories/mfsa2026-33/
- https://www.mozilla.org/security/advisories/mfsa2026-34/
- https://bdu.fstec.ru/vul/2026-06953

87

Краткое описание: Выполнение произвольного кода в Firefox

Идентификатор уязвимости: CVE-2026-6786
BDU:2026-06954

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Firefox: до 150
Firefox ESR: до 140.10
Thunderbird: до 150
Thunderbird ESR: до 140.10

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: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://www.mozilla.org/security/advisories/mfsa2026-30/
- https://www.mozilla.org/security/advisories/mfsa2026-32/
- https://www.mozilla.org/security/advisories/mfsa2026-33/
- https://www.mozilla.org/security/advisories/mfsa2026-34/
- https://bdu.fstec.ru/vul/2026-06954

88

Краткое описание: Обход безопасности в Firefox

Идентификатор уязвимости: CVE-2026-6772
BDU:2026-06955

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

Уязвимый продукт: Firefox: до 150
Firefox ESR: до 115.35
Thunderbird: до 150

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 7.5 AV:N/AC: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: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://www.mozilla.org/security/advisories/mfsa2026-30/
- https://www.mozilla.org/security/advisories/mfsa2026-31/
- https://www.mozilla.org/security/advisories/mfsa2026-32/
- https://www.mozilla.org/security/advisories/mfsa2026-33/
- https://www.mozilla.org/security/advisories/mfsa2026-34/
- https://bdu.fstec.ru/vul/2026-06955

89

Краткое описание: Отказ в обслуживании в Firefox

Идентификатор уязвимости: CVE-2026-6773
BDU:2026-06958

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

Уязвимый продукт: Firefox: до 150
Thunderbird: до 150

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://www.mozilla.org/security/advisories/mfsa2026-30/
- https://www.mozilla.org/security/advisories/mfsa2026-33/
- https://bdu.fstec.ru/vul/2026-06958

90

Краткое описание: Отказ в обслуживании в Firefox

Идентификатор уязвимости: CVE-2026-6781
BDU:2026-06960

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

Уязвимый продукт: Firefox: до 150
Thunderbird: до 150

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://www.mozilla.org/security/advisories/mfsa2026-30/
- https://www.mozilla.org/security/advisories/mfsa2026-33/
- https://bdu.fstec.ru/vul/2026-06960

91

Краткое описание: Выполнение произвольного кода в xrdp

Идентификатор уязвимости: CVE-2026-35512
BDU:2026-06984

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

Уязвимый продукт: xrdp: до 0.10.6

Категория уязвимого продукта: Не определено

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: 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: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://github.com/neutrinolabs/xrdp/security/advisories/GHSA-jg6p-7fg8-9hh6
- https://bdu.fstec.ru/vul/2026-06984

Краткое описание: Выполнение произвольного кода в Firefox

Идентификатор уязвимости: CVE-2026-6784
BDU:2026-06957

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Firefox: до 150
Thunderbird: до 150

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://www.mozilla.org/security/advisories/mfsa2026-30/
- https://www.mozilla.org/security/advisories/mfsa2026-33/
- https://bdu.fstec.ru/vul/2026-06957

93

Краткое описание: Выполнение произвольного кода в xrdp

Идентификатор уязвимости: CVE-2026-32107
BDU:2026-06986

Идентификатор программной ошибки: CWE-273 Некорректная проверка выполнения сброса привилегий

Уязвимый продукт: xrdp: до 0.10.6

Категория уязвимого продукта: Не определено

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: 8.8 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: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://github.com/neutrinolabs/xrdp/security/advisories/GHSA-p5m6-7m43-pjv9
- https://bdu.fstec.ru/vul/2026-06986

94

Краткое описание: Выполнение произвольного кода в Gitlab

Идентификатор уязвимости: CVE-2026-6073
BDU:2026-06916

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

Уязвимый продукт: Gitlab: от 18.11 до 18.11.3

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: 8.7 AV:N/AC:L/PR:L/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: 2026-05-18 / 2026-05-18

Ссылки на источник:

- https://docs.gitlab.com/releases/
- https://hackerone.com/reports/3655677
- https://bdu.fstec.ru/vul/2026-06916

95

Краткое описание: Выполнение произвольного кода в Gitlab

Идентификатор уязвимости: CVE-2026-7481
BDU:2026-06917

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

Уязвимый продукт: Gitlab: от 16.4 до 18.9.7

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: 8.7 AV:N/AC:L/PR:L/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: 2026-05-18 / 2026-05-18

Ссылки на источник:

- https://about.gitlab.com/releases/2026/05/13/patch-release-gitlab-18-11-3-released/
- https://hackerone.com/reports/3697379
- https://bdu.fstec.ru/vul/2026-06917

96

Краткое описание: Выполнение произвольного кода в Adobe Premiere Pro

Идентификатор уязвимости: CVE-2026-34637
BDU:2026-06929

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Premiere Pro: до 25.6.4 включительно
Adobe Premiere: до 26.0.2 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-13 / 2026-05-13

Ссылки на источник:

- https://helpx.adobe.com/security/products/premiere_pro/apsb26-46.html
- https://bdu.fstec.ru/vul/2026-06929

Краткое описание: Обход безопасности в Tomcat

Идентификатор уязвимости: CVE-2026-24880
BDU:2026-06932

Идентификатор программной ошибки: CWE-444 Некорректная интерпретация HTTP-запросов (несанкционированные HTTP-запросы)

Уязвимый продукт: Tomcat: от 7.0.0 до 7.0.109
РЕД ОС: 8.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Обход безопасности

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

97 **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: 2026-05-15 / 2026-05-15

Ссылки на источник:

- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-24880
- https://github.com/apache/tomcat/commit/2cb06c34f661ca42f7570bbcc21e99806184bcc5
- https://github.com/apache/tomcat
- https://lists.apache.org/thread/2c682qnlg2tv4o5knlggqbl9yc2gb5sn
- https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.116
- https://github.com/apache/tomcat/commit/fde1a8235fb73125217bd41e162aa0a113f33552
- https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.20
- https://www.herodevs.com/vulnerability-directory/cve-2026-24880
- https://github.com/apache/tomcat/commit/6d478dbe18b7c4bb671c30fedf130309b0dab77c

- https://github.com/apache/tomcat/commit/1b586d6aa8ae65726da5fa8799427b5d4718478a
- https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.53
- https://www.openwall.com/lists/oss-security/2026/04/09/20
- https://bdu.fstec.ru/vul/2026-06932

98

Краткое описание: Отказ в обслуживании в xrdp

Идентификатор уязвимости: CVE-2026-32623
BDU:2026-06987

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

Уязвимый продукт: xrdp: до 0.10.1 включительно

Категория уязвимого продукта: Не определено

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://github.com/neutrinolabs/xrdp/security/advisories/GHSA-phw3-qp59-x2v4
- https://bdu.fstec.ru/vul/2026-06987

99

Краткое описание: Отказ в обслуживании в xrdp

Идентификатор уязвимости: CVE-2026-33689
BDU:2026-06991

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: xrdp: до 0.10.6

Категория уязвимого продукта: Не определено

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://github.com/neutrinolabs/xrdp/security/advisories/GHSA-92mr-6wpp-27jj
- https://bdu.fstec.ru/vul/2026-06991

100

Краткое описание: Обход безопасности в PAN-OS

Идентификатор уязвимости: CVE-2026-0265
BDU:2026-07004

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: PAN-OS: до 10.2.18-h6

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 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: 2026-05-18 / 2026-05-18

Ссылки на источник:

- https://security.paloaltonetworks.com/CVE-2026-0265
- https://github.com/tstephens1080/palo-alto-cve-2026-0265-checker
- https://bdu.fstec.ru/vul/2026-07004

101

Краткое описание: Обход безопасности в Catalyst SD-WAN Manager

Идентификатор уязвимости: CVE-2026-20224
BDU:2026-07003

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Catalyst SD-WAN Manager: от 26.1 до 26.1.1.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2026-05-18 / 2026-05-18

Ссылки на источник:

- https://github.com/fevar54/CVE-2026-20224---XXE-Injection-en-Cisco-Catalyst-SD-WAN-Manager
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW
- https://bdu.fstec.ru/vul/2026-07003

102

Краткое описание: Подделка запросов на стороне сервера в DNN

Идентификатор уязвимости: CVE-2025-32372
BDU:2026-07002

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

Уязвимый продукт: DNN: до 9.13.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Подделка запросов на стороне сервера

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-05-18 / 2026-05-18

Ссылки на источник:

- https://github.com/dnnsoftware/Dnn.Platform/security/advisories/GHSA-3f7v-qx94-666m
- https://bdu.fstec.ru/vul/2026-07002

103

Краткое описание: Отказ в обслуживании в xrdp

Идентификатор уязвимости: CVE-2026-33516
BDU:2026-06990

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: xrdp: до 0.10.6

Категория уязвимого продукта: Не определено

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-04-22 / 2026-04-22

Ссылки на источник:

- https://github.com/neutrinolabs/xrdp/security/advisories/GHSA-rvh9-9wm3-28c7
- https://bdu.fstec.ru/vul/2026-06990

104

Краткое описание: Получение конфиденциальной информации в Gitlab

Идентификатор уязвимости: CVE-2026-1322
BDU:2026-07012

Идентификатор программной ошибки: CWE-840 Ошибки в бизнес-логике

Уязвимый продукт: Gitlab: от 16.0 до 18.9.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.1 AV:N/AC:L/PR: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: 2026-05-18 / 2026-05-18

Ссылки на источник:

- https://about.gitlab.com/releases/2026/05/13/patch-release-gitlab-18-11-3-released/
- https://hackerone.com/reports/3508895
- https://bdu.fstec.ru/vul/2026-07012

105

Краткое описание: Отказ в обслуживании в Gitlab

Идентификатор уязвимости: CVE-2026-1184
BDU:2026-07011

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Gitlab: от 11.9 до 18.9.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 AV:N/AC: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: 2026-05-18 / 2026-05-18

Ссылки на источник:

- https://about.gitlab.com/releases/2026/05/13/patch-release-gitlab-18-11-3-released/
- https://hackerone.com/reports/3515842
- https://bdu.fstec.ru/vul/2026-07011

106

Краткое описание: Отказ в обслуживании в Gitlab

Идентификатор уязвимости: CVE-2025-14870
BDU:2026-07010

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

Уязвимый продукт: Gitlab: от 18.5 до 18.9.7

Категория уязвимого продукта: Прикладное программное обеспечение

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: 2026-05-18 / 2026-05-18

Ссылки на источник:

- https://about.gitlab.com/releases/2026/05/13/patch-release-gitlab-18-11-3-released/
- https://hackerone.com/reports/3446641
- https://bdu.fstec.ru/vul/2026-07010

Краткое описание: Выполнение произвольного кода в WebdriverIO

Идентификатор уязвимости: CVE-2026-25244
BDU:2026-07092

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

Уязвимый продукт: WebdriverIO: до 9.24.0

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.

107

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: 2026-05-20 / 2026-05-20

Ссылки на источник:

- https://github.com/webdriverio/webdriverio/blob/ea0e3e00288abced4c739ff9e46c46977b7cdbd2/packages/wdio-browserstack-service/src/testorchestration/helpers.ts#L204
- https://github.com/webdriverio/webdriverio/releases/tag/v9.24.0
- https://github.com/webdriverio/webdriverio/security/advisories/GHSA-5c46-x3qw-q7j7
- https://bdu.fstec.ru/vul/2026-07092

Краткое описание: Повышение привилегий в Photoshop

Идентификатор уязвимости: CVE-2026-34632
BDU:2026-07112

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: Photoshop: -

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.

108

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: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://talosintelligence.com/vulnerability_reports/TALOS-2025-2274
- https://feedly.com/cve/CVE-2026-34632
- https://helpx.adobe.com/security/products/photoshop/apsb26-40.html
- https://bdu.fstec.ru/vul/2026-07112

109

Краткое описание: Отказ в обслуживании в Ubuntu

Идентификатор уязвимости: CVE-2026-35058
BDU:2026-07108

Идентификатор программной ошибки: CWE-617 Несанкционированный вызов утверждения

Уязвимый продукт: Ubuntu: 26.04 LTS
OpenVPN: от 2.7_alpha1 до 2.7.2

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://talosintelligence.com/vulnerability_reports/TALOS-2026-2381
- https://community.openvpn.net/Security%20Announcements/CVE-2026-35058
- https://security-tracker.debian.org/tracker/CVE-2026-35058
- https://ubuntu.com/security/CVE-2026-35058
- https://bdu.fstec.ru/vul/2026-07108

110

Краткое описание: Повышение привилегий в Microsoft Malware Protection Engine

Идентификатор уязвимости: CVE-2026-41091
BDU:2026-07110

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

Уязвимый продукт: Microsoft Malware Protection Engine: от 1.1.26030.3008 до 1.1.26040.8

Категория уязвимого продукта: Операционные системы Microsoft 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: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41091
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-41091
- https://github.com/0xBlackash/CVE-2026-41091
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-07110

111

Краткое описание: Выполнение произвольного кода в РЕД ОС

Идентификатор уязвимости: CVE-2026-29047
BDU:2026-07154

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

Уязвимый продукт: РЕД ОС: 8.0
GLPI: от 11.0.0 до 11.0.6

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 2026-05-20 / 2026-05-20

Ссылки на источник:

- https://github.com/glpi-project/glpi/security/advisories/GHSA-3m49-qf92-vccr
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-29047
- https://bdu.fstec.ru/vul/2026-07154

112

Краткое описание: Выполнение произвольного кода в РЕД ОС

Идентификатор уязвимости: CVE-2026-26263
BDU:2026-07155

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

Уязвимый продукт: РЕД ОС: 8.0
GLPI: до 10.0.6

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 9.8 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: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://github.com/glpi-project/glpi/security/advisories/GHSA-346p-qj3v-9rxj
- https://redos.red-soft.ru/search/?iblock_id=&q=CVE-2026-26263
- https://bdu.fstec.ru/vul/2026-07155

113

Краткое описание: Повышение привилегий в Windows Admin Center in Azure Portal

Идентификатор уязвимости: CVE-2026-41086
BDU:2026-07128

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Windows Admin Center in Azure Portal: до 2.6.7

Категория уязвимого продукта: Операционные системы Microsoft и их 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: 2026-05-22 / 2026-05-22

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41086
- https://bdu.fstec.ru/vul/2026-07128

Краткое описание: Отказ в обслуживании в FreeBSD

Идентификатор уязвимости: CVE-2026-45250
BDU:2026-07113

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: FreeBSD: до 14.3-RELEASE-p14

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.

114

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: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://www.freebsd.org/security/advisories/FreeBSD-SA-26:18.setcred.asc
- https://www.reddit.com/r/freebsd/comments/1tjaceg/20260520_freebsd_errata_notice_and_seven_security/
- https://github.com/venglin/setcred
- https://github.com/advisories/GHSA-qr94-c32q-xh3q
- https://seclists.org/oss-sec/2026/q2/639
- https://bdu.fstec.ru/vul/2026-07113

115

Краткое описание: Выполнение произвольного кода в Windows 10 1809

Идентификатор уязвимости: CVE-2026-40415
BDU:2026-07120

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-22 / 2026-05-22

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40415
- https://bdu.fstec.ru/vul/2026-07120

116

Краткое описание: Повышение привилегий в Windows 10 1607

Идентификатор уязвимости: CVE-2026-40399
BDU:2026-07122

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-22 / 2026-05-22

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40399
- https://bdu.fstec.ru/vul/2026-07122

117

Краткое описание: Повышение привилегий в Windows 10 1607

Идентификатор уязвимости: CVE-2026-40397
BDU:2026-07124

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-22 / 2026-05-22

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40397
- https://bdu.fstec.ru/vul/2026-07124

118

Краткое описание: Выполнение произвольного кода в PT Dephaze

Идентификатор уязвимости: BDU:2026-07126

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

Уязвимый продукт: PT Dephaze: до 2025.3.0.1 включительно

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: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: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://ptsecurity.com/research/threatscape/PT-2026-04/
- https://bdu.fstec.ru/vul/2026-07126

119

Краткое описание: Выполнение произвольного кода в PT Dephaze

Идентификатор уязвимости: BDU:2026-07127

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

Уязвимый продукт: PT Dephaze: до 2025.3.0.1 включительно

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: 8.5 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: 2026-05-21 / 2026-05-21

Ссылки на источник:

- https://ptsecurity.com/research/threatscape/PT-2026-05/
- https://bdu.fstec.ru/vul/2026-07127

120

Краткое описание: Повышение привилегий в Windows 10 1607

Идентификатор уязвимости: CVE-2026-40408
BDU:2026-07121

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9140
Windows 10 1809: до 10.0.17763.8755
Windows 10 21H2: до 10.0.19044.7291
Windows 10 22H2: до 10.0.19045.7291
Windows 11 23H2: до 10.0.22631.7079
Windows 11 24H2: до 10.0.26100.8390
Windows Server 2012: до 6.2.9200.26079
Windows Server 2012 R2: до 6.3.9600.23181
Windows Server 2012 (Server Core installation): до 6.2.9200.26079
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23181
Windows Server 2016: до 10.0.14393.9140
Windows Server 2016 (Server Core installation): до 10.0.14393.9140
Windows Server 2019: до 10.0.17763.8755
Windows Server 2019 (Server Core installation): до 10.0.17763.8755
Windows Server 2022: до 10.0.20348.5074
Windows Server 2022, 23H2 Edition (Server Core installation): до 10.0.25398.2330
Windows Server 2022 (Server Core installation): до 10.0.20348.5074
Windows Server 2025: до 10.0.26100.32772
Windows Server 2025 (Server Core installation): до 10.0.26100.32772
Windows 11 25H2: до 10.0.26200.8390
Windows 11 26H1: до 10.0.28000.2113

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: 2026-05-22 / 2026-05-22

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40408
- https://bdu.fstec.ru/vul/2026-07121

121

Краткое описание: Получение конфиденциальной информации в РЕД ОС

Идентификатор уязвимости: CVE-2026-32633
BDU:2026-07159

Идентификатор программной ошибки: CWE-522 Недостаточно надежная защита учетных данных

Уязвимый продукт: РЕД ОС: 8.0
Glances: до 4.5.2

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 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: 2026-05-20 / 2026-05-20

Ссылки на источник:

- https://github.com/nicolargo/glances/security/advisories/GHSA-r297-p3v4-wp8m
- https://github.com/nicolargo/glances/releases/tag/v4.5.2
- https://github.com/nicolargo/glances
- https://github.com/nicolargo/glances/commit/879ef8688ffa1630839549751d3c7ef9961d361e
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-glances-cve-2026-32633-8.0/?sphrase_id=1504993
- https://bdu.fstec.ru/vul/2026-07159

Краткое описание: Выполнение произвольного кода в РЕД ОС

Идентификатор уязвимости: CVE-2026-32611
BDU:2026-07160

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

Уязвимый продукт: РЕД ОС: 8.0
Glances: до 4.5.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

122

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: 2026-05-20 / 2026-05-20

Ссылки на источник:

- https://github.com/nicolargo/glances/releases/tag/v4.5.2
- https://github.com/nicolargo/glances
- https://github.com/nicolargo/glances/commit/63b7da28895249d775202d639e5531ba63491a5c
- https://github.com/nicolargo/glances/security/advisories/GHSA-49g7-2ww7-3vf5
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-glances-cve-2026-32611-8.0/?sphrase_id=1504986
- https://bdu.fstec.ru/vul/2026-07160

123

Краткое описание: Получение конфиденциальной информации в РЕД ОС

Идентификатор уязвимости: CVE-2026-32610
BDU:2026-07230

Идентификатор программной ошибки: CWE-1004 Отсутствие флага HttpOnly у конфиденциальных куки-параметров

Уязвимый продукт: РЕД ОС: 8.0
Glances: до 4.5.3

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-05-18 / 2026-05-18

Ссылки на источник:

- https://github.com/nicolargo/glances
- https://github.com/nicolargo/glances/commit/4465169b71d93991f1e49740fe02428291099832
- https://github.com/nicolargo/glances/releases/tag/v4.5.2
- https://github.com/nicolargo/glances/security/advisories/GHSA-9jfm-9rc6-2hfq
- https://redos.red-soft.ru/search/?iblock_id=24&q=CVE-2026-32610
- https://bdu.fstec.ru/vul/2026-07230

124

Краткое описание: Получение конфиденциальной информации в РЕД ОС

Идентификатор уязвимости: CVE-2026-32634
BDU:2026-07194

Идентификатор программной ошибки: CWE-542 НЕ РЕКОМЕНДУЕТСЯ: Разглашение информации, связанное с файлами журналов очистки

Уязвимый продукт: РЕД ОС: 8.0
Glances: до 4.5.2

Категория уязвимого продукта: Unix-подобные операционные системы и их 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: 8.1 AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-05-22 / 2026-05-22

Ссылки на источник:

- https://github.com/nicolargo/glances/security/advisories/GHSA-vx5f-957p-qpvm
- https://github.com/nicolargo/glances/releases/tag/v4.5.2
- https://github.com/nicolargo/glances
- https://github.com/nicolargo/glances/commit/61d38eec521703e41e4933d18d5a5ef6f854abd5
- https://redos.red-soft.ru/support/secure/uyazvimosti-red-os-8-0/uyazvimost-glances-cve-2026-32634-8.0/?sphrase_id=1507269
- https://security-tracker.debian.org/tracker/CVE-2026-32634
- https://bdu.fstec.ru/vul/2026-07194