

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

Бюллетень об уязвимостях программного обеспечения

VULN.2026-10-12.1 | 12 октября 2026 года

TLP: WHITE



Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2026-94127	F5 BIG-IP Access Policy Manager	Сетевой	ACE	2026-09-22	✓
2	Высокая	CVE-2026-20250	Cisco Secure FTD и Cisco Secure Firewall ASA	Сетевой	DoS	2026-09-23	✓
3	Критическая	CVE-2026-20284	Cisco Identity Services Engine (ISE)	Сетевой	DoS	2026-09-23	✓
4	Высокая	CVE-2026-20247	Cisco Identity Services Engine (ISE)	Сетевой	ACE	2026-09-23	✓
5	Высокая	CVE-2026-20295	Cisco Secure Firewall Management Center	Сетевой	DoS	2026-09-23	✓
6	Высокая	CVE-2026-20323	Cisco Secure Firewall Management Center	Смежная сеть	DoS	2026-09-23	✓
7	Высокая	CVE-2026-20249	Cisco Secure FTD и Cisco Secure Firewall ASA	Сетевой	DoS	2026-09-23	✓
8	Высокая	CVE-2026-20154	Cisco Secure FTD и Cisco Secure Firewall ASA	Сетевой	DoS	2026-09-23	✓
9	Критическая	CVE-2026-76420	Cisco Secure Firewall Management Center	Сетевой	PE	2026-09-23	✓
10	Высокая	CVE-2026-20135	Cisco Secure Firewall Threat Defense (FTD)	Сетевой	DoS	2026-09-23	✓
11	Критическая	CVE-2026-76443	Cisco Secure Email и Web Manager	Сетевой	ACE	2026-09-23	✓

12	Критическая	CVE-2026-76441	Cisco Secure Email and Web Manager	Сетевой	SB	2026-09-23	✓
13	Критическая	CVE-2026-76440	Cisco Secure Email and Web Manager	Сетевой	ACE	2026-09-23	✓
14	Критическая	CVE-2026-20353	Cisco Secure Email and Web Manager	Сетевой	DoS	2026-09-23	✓
15	Высокая	CVE-2026-20352	Cisco Identity Services Engine (ISE)	Сетевой	DoS	2026-09-23	✓
16	Критическая	CVE-2026-20234	Cisco Identity Services Engine	Сетевой	OSI	2026-09-23	✓
17	Критическая	CVE-2026-20305	Cisco Identity Services Engine (ISE)	Сетевой	ACE	2026-09-23	✓
18	Критическая	CVE-2026-20306	Cisco Identity Services Engine (ISE)	Сетевой	ACE	2026-09-23	✓
19	Критическая	CVE-2026-20307	Cisco Identity Services Engine (ISE)	Сетевой	ACE	2026-09-23	✓
20	Высокая	CVE-2026-76442	Cisco Secure Email and Web Manager и Cisco Secure Email Gateway	Сетевой	DoS	2026-09-23	✓
21	Критическая	CVE-2026-82078	PaperCut MF	Сетевой	ACE	2026-09-23	✓
22	Критическая	CVE-2026-93616	Security Management Server	Сетевой	ACE	2026-09-23	✓
23	Критическая	CVE-2026-58240	SAP NetWeaver	Сетевой	ACE	2026-09-23	✓
24	Высокая	CVE-2026-81578	PaperCut MF	Сетевой	CI	2026-09-23	✓
25	Критическая	CVE-2026-94545	Next.js	Сетевой	ACE	2026-09-24	✓
26	Высокая	CVE-2026-77422	JLine	Сетевой	DoS	2026-09-25	✓

27	Высокая	CVE-2026-6668	PgBouncer	Сетевой	DoS	2026-09-25	✓
28	Высокая	CVE-2026-19888	PgBouncer	Сетевой	DoS	2026-09-25	✓
29	Критическая	CVE-2026-93577	Gitlab	Сетевой	ACE	2026-09-25	✓
30	Критическая	CVE-2026-89078	Gitlab	Сетевой	ACE	2026-09-25	✓
31	Критическая	CVE-2026-88772	NetScaler Gateway	Сетевой	ACE	2026-09-28	✓
32	Критическая	BDU:2026-15495	tac_plus	Сетевой	ACE	2026-09-25	✓
33	Критическая	CVE-2026-88771	NetScaler Gateway	Сетевой	ACE	2026-09-28	✓
34	Высокая	CVE-2026-83997	Windows Message Queuing	Сетевой	ACE	2026-09-25	✓
35	Высокая	CVE-2026-83986	Windows Biometric Service	Локальный	PE	2026-09-25	✓
36	Высокая	CVE-2026-83987	Windows Biometric Service	Локальный	PE	2026-09-25	✓
37	Высокая	CVE-2026-83988	Windows Biometric Service	Локальный	PE	2026-09-25	✓
38	Высокая	CVE-2026-83989	Windows Services for NFS ONCRPC XDR Driver	Сетевой	DoS	2026-09-25	✓
39	Высокая	CVE-2026-83992	Windows Imaging Component	Сетевой	ACE	2026-09-25	✓
40	Высокая	CVE-2026-83995	Windows NTFS	Локальный	PE	2026-09-25	✓
41	Высокая	CVE-2026-83996	Windows Error Reporting	Локальный	PE	2026-09-25	✓

42	Высокая	CVE-2026-81951	Microsoft Excel	Локальный	ACE	2026-09-28	✓
43	Высокая	CVE-2026-81950	Microsoft Excel	Локальный	ACE	2026-09-28	✓
44	Высокая	CVE-2026-81949	Microsoft Excel	Локальный	ACE	2026-09-28	✓
45	Высокая	CVE-2026-81948	Microsoft Excel	Локальный	ACE	2026-09-28	✓
46	Высокая	CVE-2026-81947	Office Online Server	Локальный	ACE	2026-09-28	✓
47	Высокая	CVE-2026-81397	Microsoft Excel	Локальный	ACE	2026-09-28	✓
48	Высокая	CVE-2026-81396	Microsoft Excel	Локальный	ACE	2026-09-28	✓
49	Высокая	CVE-2026-81388	Microsoft Excel	Локальный	ACE	2026-09-28	✓
50	Высокая	CVE-2026-81386	Microsoft Excel	Локальный	ACE	2026-09-28	✓
51	Высокая	CVE-2026-81353	Microsoft HEIF Image Extension	Локальный	ACE	2026-09-28	✓
52	Высокая	CVE-2026-80097	Microsoft Authenticator	Локальный	PE	2026-09-28	✓
53	Высокая	CVE-2026-80081	Microsoft Office PowerPoint	Сетевой	ACE	2026-09-28	✓
54	Высокая	CVE-2026-80080	Microsoft Office Word	Сетевой	ACE	2026-09-28	✓
55	Высокая	CVE-2026-78525	Microsoft Office Outlook	Сетевой	ACE	2026-09-28	✓
56	Высокая	CVE-2026-78524	Microsoft Office	Сетевой	ACE	2026-09-28	✓

57	Высокая	CVE-2026-81952	Microsoft Word	Сетевой	ACE	2026-09-28	✓
58	Высокая	CVE-2026-81953	Microsoft Excel	Локальный	ACE	2026-09-28	✓
59	Высокая	CVE-2026-81398	Microsoft Excel	Локальный	ACE	2026-09-28	✓
60	Высокая	CVE-2026-81956	Office Online Server	Локальный	ACE	2026-09-28	✓
61	Высокая	CVE-2026-81954	Microsoft Excel	Локальный	ACE	2026-09-28	✓
62	Высокая	CVE-2026-83990	Microsoft Graphics Component	Локальный	PE	2026-09-28	✓
63	Высокая	CVE-2026-81352	Microsoft Web Media Extensions	Сетевой	ACE	2026-09-28	✓
64	Высокая	CVE-2026-81385	Microsoft Office Publisher	Сетевой	ACE	2026-09-28	✓
65	Высокая	CVE-2026-78526	Microsoft Office Word	Сетевой	ACE	2026-09-28	✓
66	Высокая	CVE-2026-81955	Windows Graphics Component	Сетевой	ACE	2026-09-28	✓
67	Высокая	CVE-2026-81960	Microsoft Excel	Локальный	ACE	2026-09-28	✓
68	Высокая	CVE-2026-81957	Microsoft Excel	Локальный	ACE	2026-09-28	✓
69	Высокая	CVE-2026-81959	Microsoft Excel	Локальный	ACE	2026-09-28	✓
70	Высокая	CVE-2026-72993	Windows Biometric Service	Локальный	PE	2026-09-29	✓
71	Высокая	CVE-2026-72992	Windows Biometric Service	Локальный	PE	2026-09-29	✓

72	Высокая	CVE-2026-72991	Windows Biometric Service	Локальный	PE	2026-09-29	✓
73	Высокая	CVE-2026-72989	Windows Failover Cluster	Сетевой	OSI	2026-09-29	✓
74	Высокая	CVE-2026-72988	Windows Biometric Service	Локальный	PE	2026-09-29	✓
75	Высокая	CVE-2026-72987	Windows DNS	Сетевой	ACE	2026-09-29	✓
76	Высокая	CVE-2026-72986	Windows Graphic Fonts	Сетевой	ACE	2026-09-29	✓
77	Критическая	CVE-2026-81376	Visual Studio Code	Сетевой	SB	2026-09-28	✓
78	Высокая	CVE-2026-72973	Microsoft Office Word	Сетевой	ACE	2026-09-29	✓
79	Высокая	CVE-2026-72995	Windows Biometric Service	Локальный	PE	2026-09-28	✓
80	Высокая	CVE-2026-72994	Windows Biometric Service	Локальный	PE	2026-09-29	✓
81	Высокая	CVE-2026-72981	Windows IP Helper	Сетевой	ACE	2026-09-29	✓
82	Высокая	CVE-2026-72990	Windows Biometric Service	Локальный	PE	2026-09-28	✓
83	Критическая	CVE-2026-68839	Windows USB Mass Storage Class Driver	Сетевой	ACE	2026-09-29	✓
84	Высокая	CVE-2026-65660	Microsoft SharePoint Server	Сетевой	ACE	2026-09-28	✓
85	Критическая	CVE-2026-69641	Microsoft Exchange Server	Сетевой	PE	2026-09-29	✓
86	Критическая	CVE-2026-69356	Microsoft Exchange Server	Сетевой	SB	2026-09-29	✓

87	Критическая	CVE-2026-69276	Microsoft UxTheme Library	Сетевой	ACE	2026-09-29	✓
88	Высокая	CVE-2026-46174	Linux	Локальный	ACE	2026-09-30	✓
89	Высокая	CVE-2026-46166	Linux	Смежная сеть	ACE	2026-09-30	✓
90	Высокая	CVE-2026-46156	Linux	Смежная сеть	ACE	2026-09-30	✓
91	Высокая	CVE-2026-46152	Linux	Смежная сеть	ACE	2026-09-30	✓
92	Критическая	CVE-2026-46137	Linux	Сетевой	ACE	2026-09-30	✓
93	Высокая	CVE-2026-46128	Linux	Смежная сеть	ACE	2026-09-30	✓
94	Высокая	CVE-2026-46102	Linux	Сетевой	DoS	2026-09-30	✓
95	Высокая	CVE-2026-46097	Linux	Смежная сеть	ACE	2026-09-30	✓
96	Высокая	CVE-2026-46096	Linux	Смежная сеть	ACE	2026-09-30	✓
97	Высокая	CVE-2026-46085	Linux	Сетевой	DoS	2026-09-30	✓
98	Высокая	CVE-2026-46198	Linux	Смежная сеть	ACE	2026-09-30	✓
99	Высокая	CVE-2026-46125	Linux	Смежная сеть	ACE	2026-09-30	✓

100	Высокая	CVE-2026-46212	Linux	Смежная сеть	ACE	2026-09-30	✓
101	Критическая	CVE-2026-20357	Crosswork Data Gateway	Сетевой	ACE	2026-09-30	✓
102	Высокая	CVE-2026-46229	Linux	Смежная сеть	ACE	2026-09-30	✓
103	Критическая	CVE-2026-62815	Microsoft QUIC	Сетевой	ACE	2026-09-30	✓
104	Высокая	CVE-2026-46227	Linux	Локальный	ACE	2026-09-30	✓
105	Критическая	CVE-2026-20318	Cisco Secure Workload	Сетевой	ACE	2026-09-30	✓
106	Высокая	CVE-2026-46058	Linux	Локальный	ACE	2026-09-30	✓
107	Критическая	CVE-2026-20358	Cisco Crosswork Data Gateway	Сетевой	ACE	2026-09-30	✓
108	Критическая	CVE-2026-20359	Cisco Crosswork Data Gateway	Сетевой	ACE	2026-09-30	✓
109	Высокая	CVE-2026-46240	Linux	Локальный	ACE	2026-09-30	✓
110	Высокая	CVE-2026-46232	Linux	Смежная сеть	DoS	2026-09-30	✓
111	Критическая	CVE-2026-20030	Cisco Crosswork Data Gateway	Сетевой	ACE	2026-09-30	✓
112	Высокая	CVE-2026-46037	Linux	Сетевой	DoS	2026-09-30	✓
113	Высокая	CVE-2026-45989	Linux	Смежная сеть	ACE	2026-09-30	✓

114	Критическая	CVE-2026-19516	Grafana MCP Server	Сетевой	RLF	2026-09-29	✓
115	Высокая	CVE-2026-27212	Swiper	Локальный	ACE	2026-09-29	✓
116	Критическая	CVE-2026-89775	Linux	Локальный	ACE	2026-09-29	✓
117	Высокая	CVE-2026-72972	Microsoft 365 Apps for Enterprise	Сетевой	ACE	2026-09-29	✓
118	Высокая	CVE-2026-72967	Windows Network Connection Broker	Локальный	PE	2026-09-29	✓
119	Высокая	CVE-2026-72965	Windows WebClient Service	Локальный	PE	2026-09-29	✓
120	Критическая	CVE-2026-69851	Microsoft Entra ID	Сетевой	PE	2026-09-30	✓
121	Высокая	CVE-2026-46024	Linux	Сетевой	DoS	2026-09-30	✓
122	Высокая	CVE-2026-46015	Linux	Локальный	ACE	2026-09-30	✓
123	Высокая	CVE-2026-46011	Linux	Локальный	ACE	2026-09-30	✓
124	Высокая	CVE-2026-46010	Linux	Сетевой	ACE	2026-09-30	✓
125	Высокая	CVE-2026-46006	Linux	Локальный	ACE	2026-09-30	✓
126	Высокая	CVE-2026-46001	Linux	Смежная сеть	ACE	2026-09-30	✓
127	Высокая	CVE-2026-46027	Linux	Сетевой	DoS	2026-09-30	✓
128	Высокая	CVE-2026-45959	Linux	Локальный	ACE	2026-09-30	✓

129	Критическая	CVE-2026-43493	Linux	Сетевой	ACE	2026-09-30	✓
130	Критическая	CVE-2026-65801	Microsoft Exchange Online	Сетевой	PE	2026-09-30	✓
131	Критическая	CVE-2026-63509	Microsoft Fabric	Сетевой	PE	2026-09-30	✓

Краткое описание: Выполнение произвольного кода в F5 BIG-IP Access Policy Manager

Идентификатор уязвимости: CVE-2026-94127

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

Уязвимый продукт: 17.1.0 – до Hotfix-BIGIP-17.1.3.5.0.41.14-ENG;
17.5.0 – до Hotfix-BIGIP-17.5.1.9.0.160.12-ENG;
21.1.0 – до Hotfix-BIGIP-21.1.0.2.0.30.22-ENG.

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 0.0 AV:N/AC:L/AT:N/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: 2026-09-22 / 2026-09-23

Ссылки на источник:

- <https://my.f5.com/manage/s/article/K000162605>
- <https://nvd.nist.gov/vuln/detail/cve-2026-94127>

2

Краткое описание: Отказ в обслуживании в Cisco Secure FTD и Cisco Secure Firewall ASA

Идентификатор уязвимости: CVE-2026-20250
BDU:2026-15155

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

Уязвимый продукт: Cisco Secure Firewall Threat Defense (FTD): 10.0.0
Cisco Secure Firewall Adaptive Security Appliance (ASA): 9.24.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafld-dtld-dos-Kp57HkyO>
- <https://bdu.fstec.ru/vul/2026-15155>

3

Краткое описание: Отказ в обслуживании в Cisco Identity Services Engine (ISE)

Идентификатор уязвимости: CVE-2026-20284
BDU:2026-15154

Идентификатор программной ошибки: CWE-1001 Модели программных сбоев (вторичный кластер): использование некорректного API

Уязвимый продукт: Cisco Identity Services Engine: 3.2 Patch 11

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 9.1 AV:N/AC:L/PR:H/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: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-vul-ymSsTLCc>
- <https://bdu.fstec.ru/vul/2026-15154>

4

Краткое описание: Выполнение произвольного кода в Cisco Identity Services Engine (ISE)

Идентификатор уязвимости: CVE-2026-20247
BDU:2026-15153

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

Уязвимый продукт: Cisco Identity Services Engine: 3.3.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-sql-inj-3QTKR947>
- <https://bdu.fstec.ru/vul/2026-15153>

5

Краткое описание: Отказ в обслуживании в Cisco Secure Firewall Management Center

Идентификатор уязвимости: CVE-2026-20295
BDU:2026-15151

Идентификатор программной ошибки: CWE-789 Неконтролируемое выделение памяти

Уязвимый продукт: Cisco Secure Firewall Management Center: 10.0.1
Cisco Secure Firewall Threat Defense (FTD): 10.0.0

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmcftd-sftun-multivulns-WGVHOrN3>
- <https://bdu.fstec.ru/vul/2026-15151>

6

Краткое описание: Отказ в обслуживании в Cisco Secure Firewall Management Center

Идентификатор уязвимости: CVE-2026-20323
BDU:2026-15150

Идентификатор программной ошибки: CWE-295 Некорректная проверка сертификатов

Уязвимый продукт: Cisco Secure Firewall Management Center: 10.0.1
Cisco Secure Firewall Threat Defense (FTD): 10.0.0

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmcftd-sftun-multivulns-WGVHOrN3>
- <https://bdu.fstec.ru/vul/2026-15150>

Краткое описание: Отказ в обслуживании в Cisco Secure FTD и Cisco Secure Firewall ASA

Идентификатор уязвимости: CVE-2026-20249
BDU:2026-15156

Идентификатор программной ошибки: CWE-704 Некорректное преобразование или приведение типов

Уязвимый продукт: Cisco Secure Firewall Threat Defense (FTD): 10.0.0
Cisco Secure Firewall Adaptive Security Appliance (ASA): 9.24.1.155

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

7 Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafld-ikev2cert-dos-uWyc2xtv>
- <https://bdu.fstec.ru/vul/2026-15156>

8

Краткое описание: Отказ в обслуживании в Cisco Secure FTD и Cisco Secure Firewall ASA

Идентификатор уязвимости: CVE-2026-20154
BDU:2026-15158

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

Уязвимый продукт: Cisco Secure Firewall Threat Defense (FTD): 7.7.11
Cisco Secure Firewall Adaptive Security Appliance (ASA): 9.22.1.2

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-logging-dos-ZXXNesfN>
- <https://bdu.fstec.ru/vul/2026-15158>

9

Краткое описание: Повышение привилегий в Cisco Secure Firewall Management Center

Идентификатор уязвимости: CVE-2026-76420
BDU:2026-15160

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: Cisco Secure Firewall Management Center: 10.0.1

Категория уязвимого продукта: Средства защиты информации

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: 9.0 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: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc2-multivulns-HXgcqRG>
- <https://bdu.fstec.ru/vul/2026-15160>

10

Краткое описание: Отказ в обслуживании в Cisco Secure Firewall Threat Defense (FTD)

Идентификатор уязвимости: CVE-2026-20135
BDU:2026-15159

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Cisco Secure Firewall Threat Defense (FTD): 7.7.11

Категория уязвимого продукта: Средства защиты информации

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: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls1.3-dos-dLxwFWgF>
- <https://bdu.fstec.ru/vul/2026-15159>

11

Краткое описание: Выполнение произвольного кода в Cisco Secure Email и Web Manager

Идентификатор уязвимости: CVE-2026-76443
BDU:2026-15171

Идентификатор программной ошибки: CWE-707 Некорректное выполнение требований к структуре сообщений или данных

Уязвимый продукт: Cisco Secure Email and Web Manager: 16.0.4-010
Cisco Secure Email Gateway: 14.2.0-616

Категория уязвимого продукта: Средства защиты информации

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:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-esa-dfCrFXkm>
- <https://bdu.fstec.ru/vul/2026-15171>

12

Краткое описание: Обход безопасности в Cisco Secure Email and Web Manager

Идентификатор уязвимости: CVE-2026-76441
BDU:2026-15169

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Cisco Secure Email and Web Manager: 16.0.4-010
Cisco Secure Email Gateway: 14.2.0-616

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Нарушение авторизации.

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: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-esa-dfCrfXkm>
- <https://bdu.fstec.ru/vul/2026-15169>

13

Краткое описание: Выполнение произвольного кода в Cisco Secure Email and Web Manager

Идентификатор уязвимости: CVE-2026-76440
BDU:2026-15168

Идентификатор программной ошибки: CWE-23 Подмена относительного пути

Уязвимый продукт: Cisco Secure Email and Web Manager: 16.0.4-010
Cisco Secure Email Gateway: 14.2.0-616

Категория уязвимого продукта: Средства защиты информации

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: 9.8 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: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-esa-dfCrfXkm>
- <https://bdu.fstec.ru/vul/2026-15168>

14

Краткое описание: Отказ в обслуживании в Cisco Secure Email and Web Manager

Идентификатор уязвимости: CVE-2026-20353
BDU:2026-15167

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

Уязвимый продукт: Cisco Secure Email and Web Manager: 16.0.4-010
Cisco Secure Email Gateway: 14.2.0-616

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-esa-dfCrFXkm>
- <https://bdu.fstec.ru/vul/2026-15167>

15

Краткое описание: Отказ в обслуживании в Cisco Identity Services Engine (ISE)

Идентификатор уязвимости: CVE-2026-20352
BDU:2026-15166

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

Уязвимый продукт: Cisco Identity Services Engine: 3.3.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-RADIUS-dos-wR3hYPMw>
- <https://bdu.fstec.ru/vul/2026-15166>

16

Краткое описание: Получение конфиденциальной информации в Cisco Identity Services Engine

Идентификатор уязвимости: CVE-2026-20234
BDU:2026-15165

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

Уязвимый продукт: Cisco Identity Services Engine: 3.3.0 p1
Identity Services Engine Passive Identity Connector (ISE-PIC): 3.0.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ise-XU5EwX5T>
- <https://bdu.fstec.ru/vul/2026-15165>

Краткое описание: Выполнение произвольного кода в Cisco Identity Services Engine (ISE)

Идентификатор уязвимости: CVE-2026-20305
BDU:2026-15164

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

Уязвимый продукт: Cisco Identity Services Engine: 3.3.0
Identity Services Engine Passive Identity Connector (ISE-PIC): 3.3.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-cmd-inj-e2CuZCYZ>
- <https://bdu.fstec.ru/vul/2026-15164>

Краткое описание: Выполнение произвольного кода в Cisco Identity Services Engine (ISE)

Идентификатор уязвимости: CVE-2026-20306
BDU:2026-15163

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

Уязвимый продукт: Cisco Identity Services Engine: 3.3.0
Identity Services Engine Passive Identity Connector (ISE-PIC): 3.3.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-cmd-inj-e2CuZCYZ>
- <https://bdu.fstec.ru/vul/2026-15163>

19

Краткое описание: Выполнение произвольного кода в Cisco Identity Services Engine (ISE)

Идентификатор уязвимости: CVE-2026-20307
BDU:2026-15162

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Cisco Identity Services Engine: 3.3.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.9 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: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-se7bYU57>
- <https://bdu.fstec.ru/vul/2026-15162>

20

Краткое описание: Отказ в обслуживании в Cisco Secure Email and Web Manager и Cisco Secure Email Gateway

Идентификатор уязвимости: CVE-2026-76442
BDU:2026-15170

Идентификатор программной ошибки: CWE-1011 Авторизация

Уязвимый продукт: Cisco Secure Email and Web Manager: 16.0.4-010
Cisco Secure Email Gateway: 14.2.0-616

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-esa-dfCrfXkm>
- <https://bdu.fstec.ru/vul/2026-15170>

21

Краткое описание: Выполнение произвольного кода в PaperCut MF

Идентификатор уязвимости: CVE-2026-82078
BDU:2026-15096

Идентификатор программной ошибки: CWE-470 Использование внешних входных данных для выбора класса или кода ("небезопасное отражение")

Уязвимый продукт: PaperCut MF: до 25.0.13
PaperCut NG: до 25.0.13

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://github.com/advisories/GHSA-mjg5-wj9r-9mfx>
- <https://github.com/rapid7/metasploit-framework/pull/21842>
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=cve-2026-82078
- <https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/>
- <https://www.rapid7.com/blog/post/etr-papercut-ng-mf-critical-zero-day-exploited-in-the-wild/>
- <https://bdu.fstec.ru/vul/2026-15096>

22

Краткое описание: Выполнение произвольного кода в Security Management Server

Идентификатор уязвимости: CVE-2026-93616
BDU:2026-15065

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

Уязвимый продукт: Security Management Server: R81.10
Multi-Domain Security Management Server (MDS): R81.10

Категория уязвимого продукта: Средства защиты информации

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: 9.8 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: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://support.checkpoint.com/results/sk/sk1000171/>
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-93616
- <https://github.com/nebula031/CVE-2026-93616-PoC>
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- <https://bdu.fstec.ru/vul/2026-15065>

23

Краткое описание: Выполнение произвольного кода в SAP NetWeaver

Идентификатор уязвимости: CVE-2026-58240
BDU:2026-15064

Идентификатор программной ошибки: CWE-308 Использование однофакторной аутентификации

Уязвимый продукт: SAP NetWeaver: KERNEL 9.20

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://support.sap.com/en/my-support/knowledge-base/security-notes-news/september-2026.html>
- <https://securitybridge.com/blog/cve-2026-58240-from-patch-day-to-poc-in-96-hours/>
- <https://bdu.fstec.ru/vul/2026-15064>

24

Краткое описание: Внедрение кода в PaperCut MF

Идентификатор уязвимости: CVE-2026-81578
BDU:2026-15087

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

Уязвимый продукт: PaperCut MF: до 25.0.13
PaperCut NG: до 25.0.13

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Внедрение кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-23 / 2026-09-23

Ссылки на источник:

- <https://github.com/advisories/GHSA-44wc-j6f2-7fjr>
- <https://github.com/rapid7/metasploit-framework/pull/21842>
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-81578
- <https://www.papercut.com/kb/Main/security-bulletin-27-aug-2026-urgent-security-advisory/>
- <https://www.rapid7.com/blog/post/etr-papercut-ng-mf-critical-zero-day-exploited-in-the-wild/>
- <https://bdu.fstec.ru/vul/2026-15087>

25

Краткое описание: Выполнение произвольного кода в Next.js

Идентификатор уязвимости: CVE-2026-94545
BDU:2026-15201

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

Уязвимый продукт: Next.js: от 16.2.0 до 16.3.5 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-24 / 2026-09-24

Ссылки на источник:

- <https://github.com/vercel/satori/commit/26a52affc>
- <https://github.com/Hassham1/CVE-2026-94545-nextjs-og-poc>
- <https://vmtech.rs/en/instagram-insights/nextjs-imageresponse-svg-code-execution>
- <https://bdu.fstec.ru/vul/2026-15201>

26

Краткое описание: Отказ в обслуживании в JLine

Идентификатор уязвимости: CVE-2026-77422
BDU:2026-15230

Идентификатор программной ошибки: CWE-1018 Управление сессиями пользователей

Уязвимый продукт: JLine: до 4.3.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://github.com/jline/jline3/commit/1d5fc3099e77938b971e197211cad2d4fbb17541>
- <https://github.com/jline/jline3/commit/341ee69ccc57b7733c1b40d6993219b64b3206ae>
- <https://github.com/jline/jline3/pull/2012>
- <https://github.com/jline/jline3/pull/2018>
- <https://github.com/jline/jline3/releases/tag/4.3.1>
- <https://github.com/jline/jline3/releases/tag/jline-3.30.15>
- <https://github.com/jline/jline3/security/advisories/GHSA-r2xf-8xr9-62gw>
- <https://jline.org/docs/modules/builtins/>
- <https://bdu.fstec.ru/vul/2026-15230>

27

Краткое описание: Отказ в обслуживании в PgBouncer

Идентификатор уязвимости: CVE-2026-6668
BDU:2026-15220

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

Уязвимый продукт: PgBouncer: до 1.25.2 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://www.pgбouncer.org/changelog.html>
- <https://bdu.fstec.ru/vul/2026-15220>

28

Краткое описание: Отказ в обслуживании в PgBouncer

Идентификатор уязвимости: CVE-2026-19888
BDU:2026-15219

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: PgBouncer: от 1.11.0 до 1.25.2 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://www.pgбouncer.org/changelog.html>
- <https://bdu.fstec.ru/vul/2026-15219>

29

Краткое описание: Выполнение произвольного кода в Gitlab

Идентификатор уязвимости: CVE-2026-93577
BDU:2026-15215

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

Уязвимый продукт: Gitlab: от 19.4.0 до 19.4.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.9 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: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://hackerone.com/reports/3995696>
- <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-1-released/>
- <https://bdu.fstec.ru/vul/2026-15215>

30

Краткое описание: Выполнение произвольного кода в Gitlab

Идентификатор уязвимости: CVE-2026-89078
BDU:2026-15214

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Gitlab: от 19.4.0 до 19.4.1

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://hackerone.com/reports/4019059>
- <https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-4-1-released/>
- <https://bdu.fstec.ru/vul/2026-15214>

Краткое описание: Выполнение произвольного кода в NetScaler Gateway

Идентификатор уязвимости: CVE-2026-88772

BDU:2026-15497

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

Уязвимый продукт: NetScaler Gateway: до 13.1-64.23

NetScaler ADC FIPS: до 13.1.37.279

NetScaler ADC NDcPP: до 13.1.37.279

NetScaler ADC: до 13.1-64.23

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.0 AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://support.citrix.com/external/article/CTX697096/citrix-netscaler-adc-and-citrix-netscale.html>
- <https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway>
- <https://watchtowr.com/intelligence/citrix-netscaler-adc-citrix-netscaler-gateway-remote-code-execution-cve-2026-88771/>
- <https://cyberplace.social/@GossiTheDog/117339550445208757>
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- <https://github.com/murrez/CVE-2026-88772>
- <https://thecyberexpress.com/citrix-netscaler-cve-2026-88771-cve-2026-88772/>
- <https://bdu.fstec.ru/vul/2026-15497>

32

Краткое описание: Выполнение произвольного кода в tac_plus

Идентификатор уязвимости: BDU:2026-15495

Идентификатор программной ошибки: CWE-134 Использование форматной строки, контролируемой извне

Уязвимый продукт: tac_plus: до F4.0.4.32

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-25 / 2026-09-25

Ссылки на источник:

- https://shrubbery.net/pub/tac_plus/
- <https://mallory.ai/stories/01a0cc06-bc07-726b-a023-688642293f9c>
- <https://www.elttam.com/blog/att-cking-tacacs-to-pwn-your-network-via-a-pre-auth-rce#conclusion>
- <https://www.securitylab.ru/news/577881.php>
- <https://bdu.fstec.ru/vul/2026-15495>

33

Краткое описание: Выполнение произвольного кода в NetScaler Gateway

Идентификатор уязвимости: CVE-2026-88771
BDU:2026-15496

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: NetScaler Gateway: до 13.1-64.23
NetScaler ADC FIPS: до 13.1.37.279
NetScaler ADC NDcPP: до 13.1.37.279
NetScaler ADC: до 13.1-64.23

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://support.citrix.com/external/article/CTX697096/citrix-netscaler-adc-and-citrix-netscale.html>
- <https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway>
- <https://watchtowr.com/intelligence/citrix-netscaler-adc-citrix-netscaler-gateway-remote-code-execution-cve-2026-88771/>
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- <https://thecyberexpress.com/citrix-netscaler-cve-2026-88771-cve-2026-88772/>
- <https://bdu.fstec.ru/vul/2026-15496>

34

Краткое описание: Выполнение произвольного кода в Windows Message Queuing

Идентификатор уязвимости: CVE-2026-83997
BDU:2026-15511

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83997>
- <https://bdu.fstec.ru/vul/2026-15511>

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83986
BDU:2026-15518

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83986>
- <https://bdu.fstec.ru/vul/2026-15518>

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83987
BDU:2026-15517

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83987>
- <https://bdu.fstec.ru/vul/2026-15517>

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83988
BDU:2026-15516

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83988>
- <https://bdu.fstec.ru/vul/2026-15516>

Краткое описание: Отказ в обслуживании в Windows Services for NFS ONCRPC XDR Driver

Идентификатор уязвимости: CVE-2026-83989
BDU:2026-15515

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23398
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23398
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83989>
- <https://bdu.fstec.ru/vul/2026-15515>

Краткое описание: Выполнение произвольного кода в Windows Imaging Component

Идентификатор уязвимости: CVE-2026-83992
BDU:2026-15514

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23398
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23398
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 8.8 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: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83992>
- <https://bdu.fstec.ru/vul/2026-15514>

Краткое описание: Повышение привилегий в Windows NTFS

Идентификатор уязвимости: CVE-2026-83995
BDU:2026-15513

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23398
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23398
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83995>
- <https://bdu.fstec.ru/vul/2026-15513>

Краткое описание: Повышение привилегий в Windows Error Reporting

Идентификатор уязвимости: CVE-2026-83996
BDU:2026-15512

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23398
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23398
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 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: 2026-09-25 / 2026-09-25

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83996>
- <https://bdu.fstec.ru/vul/2026-15512>

42

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81951
BDU:2026-15450

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81951>
- <https://bdu.fstec.ru/vul/2026-15450>

43

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81950
BDU:2026-15449

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81950>
- <https://bdu.fstec.ru/vul/2026-15449>

44

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81949
BDU:2026-15448

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81949>
- <https://bdu.fstec.ru/vul/2026-15448>

45

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81948
BDU:2026-15447

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81948>
- <https://bdu.fstec.ru/vul/2026-15447>

46

Краткое описание: Выполнение произвольного кода в Office Online Server

Идентификатор уязвимости: CVE-2026-81947
BDU:2026-15446

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

Уязвимый продукт: Office Online Server: до 16.0.10417.20207
Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81947>
- <https://bdu.fstec.ru/vul/2026-15446>

47

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81397
BDU:2026-15444

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81397>
- <https://bdu.fstec.ru/vul/2026-15444>

48

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81396
BDU:2026-15443

Идентификатор программной ошибки: CWE-193 Ошибка смещения на единицу

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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:N/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81396>
- <https://bdu.fstec.ru/vul/2026-15443>

49

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81388
BDU:2026-15441

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81388>
- <https://bdu.fstec.ru/vul/2026-15441>

50

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81386
BDU:2026-15440

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81386>
- <https://bdu.fstec.ru/vul/2026-15440>

51

Краткое описание: Выполнение произвольного кода в Microsoft HEIF Image Extension

Идентификатор уязвимости: CVE-2026-81353
BDU:2026-15438

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

Уязвимый продукт: HEIF Image Extension: до 1.2.48.0

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:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81353>
- <https://bdu.fstec.ru/vul/2026-15438>

52

Краткое описание: Повышение привилегий в Microsoft Authenticator

Идентификатор уязвимости: CVE-2026-80097
BDU:2026-15437

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Authenticator: до 6.2606.4246

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80097>
- <https://bdu.fstec.ru/vul/2026-15437>

53

Краткое описание: Выполнение произвольного кода в Microsoft Office PowerPoint

Идентификатор уязвимости: CVE-2026-80081
BDU:2026-15436

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80081>
- <https://bdu.fstec.ru/vul/2026-15436>

54

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-80080
BDU:2026-15435

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Word 2016: до 16.0.5569.1000
Microsoft Office 365: до 16.113.26091433

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80080>
- <https://bdu.fstec.ru/vul/2026-15435>

55

Краткое описание: Выполнение произвольного кода в Microsoft Office Outlook

Идентификатор уязвимости: CVE-2026-78525
BDU:2026-15434

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Word 2016: до 16.0.5569.1000
Microsoft Office 365: до 16.113.26091433

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78525>
- <https://bdu.fstec.ru/vul/2026-15434>

56

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-78524
BDU:2026-15433

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1000
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78524>
- <https://bdu.fstec.ru/vul/2026-15433>

57

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2026-81952
BDU:2026-15451

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81952>
- <https://bdu.fstec.ru/vul/2026-15451>

58

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81953
BDU:2026-15452

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81953>
- <https://bdu.fstec.ru/vul/2026-15452>

59

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81398
BDU:2026-15445

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81398>
- <https://bdu.fstec.ru/vul/2026-15445>

60

Краткое описание: Выполнение произвольного кода в Office Online Server

Идентификатор уязвимости: CVE-2026-81956
BDU:2026-15454

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Office Online Server: до 16.0.10417.20207
Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81956>
- <https://bdu.fstec.ru/vul/2026-15454>

61

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81954
BDU:2026-15453

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81954>
- <https://bdu.fstec.ru/vul/2026-15453>

62

Краткое описание: Повышение привилегий в Microsoft Graphics Component

Идентификатор уязвимости: CVE-2026-83990
BDU:2026-15462

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83990>
- <https://bdu.fstec.ru/vul/2026-15462>

63

Краткое описание: Выполнение произвольного кода в Microsoft Web Media Extensions

Идентификатор уязвимости: CVE-2026-81352
BDU:2026-15461

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

Уязвимый продукт: Web Media Extensions: до 2.1.51.0

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: 8.8 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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81352>
- <https://bdu.fstec.ru/vul/2026-15461>

64

Краткое описание: Выполнение произвольного кода в Microsoft Office Publisher

Идентификатор уязвимости: CVE-2026-81385
BDU:2026-15460

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.0.14334.20906
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Publisher 2016: до 16.0.5569.1002

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81385>
- <https://bdu.fstec.ru/vul/2026-15460>

65

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-78526
BDU:2026-15459

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1002
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78526>
- <https://bdu.fstec.ru/vul/2026-15459>

Краткое описание: Выполнение произвольного кода в Windows Graphics Component

Идентификатор уязвимости: CVE-2026-81955
BDU:2026-15458

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Windows 10 1607: до 10.0.14393.9504
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23398
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23398
Windows Server 2016: до 10.0.14393.9504
Windows Server 2016 (Server Core installation): до 10.0.14393.9504
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954
Microsoft Office 365: до 16.113.26091433

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: 8.8 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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81955>
- <https://bdu.fstec.ru/vul/2026-15458>

67

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81960
BDU:2026-15457

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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:N/I:N/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81960>
- <https://bdu.fstec.ru/vul/2026-15457>

68

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81957
BDU:2026-15456

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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:N/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81957>
- <https://bdu.fstec.ru/vul/2026-15456>

69

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2026-81959
BDU:2026-15455

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Excel 2016: до 16.0.5569.1003
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2016: до 16.0.5569.1003
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Office 365: до 16.113.26091433

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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81959>
- <https://bdu.fstec.ru/vul/2026-15455>

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-72993
BDU:2026-15549

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72993>
- <https://bdu.fstec.ru/vul/2026-15549>

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-72992
BDU:2026-15550

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72992>
- <https://bdu.fstec.ru/vul/2026-15550>

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-72991
BDU:2026-15551

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72991>
- <https://bdu.fstec.ru/vul/2026-15551>

73

Краткое описание: Получение конфиденциальной информации в Windows Failover Cluster

Идентификатор уязвимости: CVE-2026-72989
BDU:2026-15552

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Windows 10 1809: до 10.0.17763.9245
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72989>
- <https://bdu.fstec.ru/vul/2026-15552>

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-72988
BDU:2026-15553

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72988>
- <https://bdu.fstec.ru/vul/2026-15553>

Краткое описание: Выполнение произвольного кода в Windows DNS

Идентификатор уязвимости: CVE-2026-72987
BDU:2026-15554

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23398
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23398
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438

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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72987>
- <https://bdu.fstec.ru/vul/2026-15554>

Краткое описание: Выполнение произвольного кода в Windows Graphic Fonts

Идентификатор уязвимости: CVE-2026-72986
BDU:2026-15555

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23398
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23398
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 8.8 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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72986>
- <https://bdu.fstec.ru/vul/2026-15555>

77

Краткое описание: Обход безопасности в Visual Studio Code

Идентификатор уязвимости: CVE-2026-81376
BDU:2026-15559

Идентификатор программной ошибки: CWE-1075 Безусловная передача управления за пределами блока переключения

Уязвимый продукт: Visual Studio Code: до 1.136.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81376>
- <https://bdu.fstec.ru/vul/2026-15559>

78

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-72973
BDU:2026-15557

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Word 2016: до 16.0.5569.1000
Microsoft Office 365: до 16.113.26091433

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72973>
- <https://bdu.fstec.ru/vul/2026-15557>

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-72995
BDU:2026-15558

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72995>
- <https://bdu.fstec.ru/vul/2026-15558>

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-72994
BDU:2026-15548

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72994>
- <https://bdu.fstec.ru/vul/2026-15548>

Краткое описание: Выполнение произвольного кода в Windows IP Helper

Идентификатор уязвимости: CVE-2026-72981
BDU:2026-15556

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23398
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23398
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72981>
- <https://bdu.fstec.ru/vul/2026-15556>

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-72990
BDU:2026-15547

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72990>
- <https://bdu.fstec.ru/vul/2026-15547>

Краткое описание: Выполнение произвольного кода в Windows USB Mass Storage Class Driver

Идентификатор уязвимости: CVE-2026-68839
BDU:2026-15545

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23398
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23398
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 9.8 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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-68839>
- <https://bdu.fstec.ru/vul/2026-15545>

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint Server

Идентификатор уязвимости: CVE-2026-65660
BDU:2026-15539

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

Уязвимый продукт: Microsoft SharePoint Server Subscription Edition: до 16.0.19725.20522
Microsoft SharePoint Enterprise Server 2016: до 16.0.5565.1001
Microsoft SharePoint Server 2019: до 16.0.10417.20198

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-28 / 2026-09-28

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65660>
- https://securityonline.info/exploited-sharepoint-rce-vulnerability/?utm_source=mastodon&utm_medium=jetpack_social
- <https://www.securityweek.com/microsoft-sharepoint-flaw-cve-2026-65660-now-exploited-in-attacks/amp/>
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- <https://bdu.fstec.ru/vul/2026-15539>

85

Краткое описание: Повышение привилегий в Microsoft Exchange Server

Идентификатор уязвимости: CVE-2026-69641
BDU:2026-15542

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Microsoft Exchange Server Subscription Edition RTM: до 15.02.2562.049
Microsoft Exchange Server 2019 Cumulative Update 15: до 15.02.1748.051
Microsoft Exchange Server 2019 Cumulative Update 14: до 15.02.1544.046
Microsoft Exchange Server 2016 Cumulative Update 23: до 15.01.2507.073

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69641>
- <https://bdu.fstec.ru/vul/2026-15542>

Краткое описание: Обход безопасности в Microsoft Exchange Server

Идентификатор уязвимости: CVE-2026-69356
BDU:2026-15543

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

Уязвимый продукт: Microsoft Exchange Server Subscription Edition RTM: до 15.02.2562.049
Microsoft Exchange Server 2019 Cumulative Update 15: до 15.02.1748.051
Microsoft Exchange Server 2019 Cumulative Update 14: до 15.02.1544.046
Microsoft Exchange Server 2016 Cumulative Update 23: до 15.01.2507.073

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69356>
- <https://bdu.fstec.ru/vul/2026-15543>

Краткое описание: Выполнение произвольного кода в Microsoft UxTheme Library

Идентификатор уязвимости: CVE-2026-69276
BDU:2026-15544

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23398
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23398
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 9.8 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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69276>
- <https://bdu.fstec.ru/vul/2026-15544>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46174
BDU:2026-15672

Идентификатор программной ошибки: CWE-653 Некорректная изоляция

Уязвимый продукт: Linux: от 6.2 до 6.6.138 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46174>
- <https://git.kernel.org/stable/c/1e23b30a80b14e5764657401ee2cca030525ae8e>
- <https://git.kernel.org/stable/c/f5bc3aef7df46eaaf423d7413ab8833f704ae576>
- <https://git.kernel.org/stable/c/251497955f2314cd39d43191e81c6151dead4c7b>
- <https://git.kernel.org/stable/c/ff6fc65b3bf73acc5ee71919154d830ad5431362>
- <https://git.kernel.org/stable/c/9109489cc8c34e50d15575a3d1ff82af586bc1aa>
- <https://git.kernel.org/stable/c/28f5ed477eef166d678d6966762cbc1de9b4f436>
- <https://git.kernel.org/stable/c/1cd85a19748b2407830376a5cbae5c0f126016e5>

- <https://git.kernel.org/linus/c21b90f77687075115d989e53a8ec5e2bb427ab1>
- <https://security-tracker.debian.org/tracker/CVE-2026-46174>
- <https://ubuntu.com/security/CVE-2026-46174>
- <https://access.redhat.com/security/cve/CVE-2026-46174>
- <https://bdu.fstec.ru/vul/2026-15672>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46166
BDU:2026-15670

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.12 до 6.12.87 включительно
Red Hat Enterprise Linux: 10.0 Extended Update Support
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46166>
- <https://git.kernel.org/stable/c/887ece6c23b49d02a6678e7a8d5ad213d75883ce>
- <https://git.kernel.org/stable/c/7577a4b8a10fab45a6ee2045ea038a5adadbb585>
- <https://git.kernel.org/stable/c/120149fb3ebcf674832ca3cafd32bedcdb686dde>
- <https://git.kernel.org/linus/ac8eb3e18f41e2cc8492cc1d358bcb786c850270>
- <https://security-tracker.debian.org/tracker/CVE-2026-46166>
- <https://ubuntu.com/security/CVE-2026-46166>
- <https://access.redhat.com/security/cve/CVE-2026-46166>

- <https://bdu.fstec.ru/vul/2026-15670>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46156
BDU:2026-15668

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Linux: от 6.19.11 до 7.0.6 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

90 **Оценка CVSSv3:** 8.0 AV:A/AC:L/PR:L/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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46156>
- <https://git.kernel.org/stable/c/07d190e4ec689d6478f7f5e36099fb9bf457e7c5>
- <https://git.kernel.org/stable/c/2cb19b06c09983727573bbe7d7430cbad480a714>
- <https://git.kernel.org/stable/c/9e1aed63a5552958ef2a9bfd699a3f990e52a77f>
- <https://git.kernel.org/stable/c/81fef1c278436e6bd68ee4ca05a0acb96e256561>
- <https://git.kernel.org/linus/8dfa2f8780e486d05b9a0ffce70b8f5fbd62053e>
- <https://security-tracker.debian.org/tracker/CVE-2026-46156>
- <https://deb.freexian.com/extended-lts/tracker/CVE-2026-46156>
- <https://ubuntu.com/security/CVE-2026-46156>

- <https://bdu.fstec.ru/vul/2026-15668>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46152
BDU:2026-15667

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

Уязвимый продукт: Linux: от 6.4 до 6.6.139 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 AV: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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46152>
- <https://git.kernel.org/stable/c/03584528bffb195e384698af9148b94e42e3f14>
- <https://git.kernel.org/stable/c/1739fc31b4de06c5c78ce0741182770fb079091e>
- <https://git.kernel.org/stable/c/e131562d6f2b958148c35c98831b007f47f0e3d3>
- <https://git.kernel.org/stable/c/3ef44f96ccc3e06e059dec57842e366f0c4b1893>
- <https://git.kernel.org/linus/7a5b81e0c87a075afd572f659d8eb68c9c4cd2ba>
- <https://security-tracker.debian.org/tracker/CVE-2026-46152>

- <https://ubuntu.com/security/CVE-2026-46152>
- <https://access.redhat.com/security/cve/CVE-2026-46152>
- <https://bdu.fstec.ru/vul/2026-15667>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46137
BDU:2026-15665

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

Уязвимый продукт: Linux: от 6.7 до 6.12.90 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.8 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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46137>
- <https://git.kernel.org/stable/c/013dcdc1961543b9a3433466bc8c79a2f4ca75b5>
- <https://git.kernel.org/stable/c/6e4710d7d8782cb61af29a7e7111ddfc38b9e1a3>
- <https://git.kernel.org/stable/c/2ad56e434199ca24a812bb353667aa1c3860f513>
- <https://git.kernel.org/stable/c/cc3c0399361efaaf7ae64262eb3f70829b1189c6>
- <https://git.kernel.org/linus/5cd6e0ad79d2615264f63929f8b457ad97ae550d>
- <https://security-tracker.debian.org/tracker/CVE-2026-46137>

- <https://deb.freexian.com/extended-lts/tracker/CVE-2026-46137>
- <https://ubuntu.com/security/CVE-2026-46137>
- <https://access.redhat.com/security/cve/CVE-2026-46137>
- <https://bdu.fstec.ru/vul/2026-15665>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46128
BDU:2026-15663

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

Уязвимый продукт: Linux: от 6.7 до 6.12.87 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46128>
- <https://git.kernel.org/stable/c/2418e4b21fb1355504d095da5d5f0a210564a43d>
- <https://git.kernel.org/stable/c/7f7ada72c07a83b46045ddfeee526bd9e2e3c8f0>
- <https://git.kernel.org/stable/c/42432b579a594b66ac32e5e7b7c26e6bc578ec89>
- <https://git.kernel.org/stable/c/24269264c3d59a49eb09b10af2c75b14f2931482>
- <https://git.kernel.org/linus/36920f30e78e69df01f9691c470b6f3ba8aebf98>
- <https://security-tracker.debian.org/tracker/CVE-2026-46128>
- <https://ubuntu.com/security/CVE-2026-46128>

- <https://bdu.fstec.ru/vul/2026-15663>

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46102
BDU:2026-15658

Идентификатор программной ошибки: CWE-401 Некорректное освобождение памяти до удаления последней ссылки (утечка памяти)

Уязвимый продукт: Linux: от 4.9 до 5.10.257 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46102>
- <https://git.kernel.org/stable/c/e9ae00490d474757c0f9c65073de83e6bb1e5a00>
- <https://git.kernel.org/stable/c/5327dad2ffe9c1b49881dd6d51ff3c6893847568>
- <https://git.kernel.org/stable/c/19ca9475f18f991735f98a22e735c43e95e6298d>
- <https://git.kernel.org/stable/c/56082f442023db9be1a5a29d4ee361de4017c0b7>
- <https://git.kernel.org/linus/fe72340daaf1af588be88056faf98965f39e6032>
- <https://security-tracker.debian.org/tracker/CVE-2026-46102>
- <https://ubuntu.com/security/CVE-2026-46102>

- <https://access.redhat.com/security/cve/CVE-2026-46102>
- <https://bdu.fstec.ru/vul/2026-15658>

95

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46097
BDU:2026-15656

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.17 до 6.18.26 включительно
Ubuntu: 26.04 LTS

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46097>
- <https://git.kernel.org/stable/c/a516d43886623e3cca5fa3446bed8fc7c7982be2>
- <https://git.kernel.org/stable/c/9f6c5e7b747d40e1c65cbfcb975857d25154c075>
- <https://git.kernel.org/linus/f5f9e07060519e2287e99019a6de1eb3ebb65c37>
- <https://ubuntu.com/security/CVE-2026-46097>
- <https://bdu.fstec.ru/vul/2026-15656>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46096
BDU:2026-15655

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

Уязвимый продукт: Linux: от 6.18.3 до 6.18.26 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46096>
- <https://git.kernel.org/stable/c/f8775d9d9062da662cc861f9ff7722a65896d4cd>
- <https://git.kernel.org/stable/c/2f434be87e256fd58254f60ddf5d7d58e775ca0b>
- <https://git.kernel.org/linus/f0f75a3d98b7959a8677b6363e23190f3018636b>
- <https://security-tracker.debian.org/tracker/CVE-2026-46096>
- <https://ubuntu.com/security/CVE-2026-46096>
- <https://bdu.fstec.ru/vul/2026-15655>

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46085
BDU:2026-15654

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: от 6.19.13 до 7.0.3 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46085>
- <https://git.kernel.org/stable/c/f1c6bd0cc786a8fa74829ce3c4b3673944a308f4>
- <https://git.kernel.org/stable/c/440d20d95e844b657a93a0b2dcc2aae155efdce6>
- <https://git.kernel.org/stable/c/f0d3efd03b2a9e0f1ffa6df8fcb264af3d494286>
- <https://git.kernel.org/stable/c/af9271eb666d07b6f65612dc160a47f7cb5220ed>
- <https://git.kernel.org/linus/def304aae2edf321d2671fd6ca766a93c21f877e>
- <https://security-tracker.debian.org/tracker/CVE-2026-46085>
- <https://ubuntu.com/security/CVE-2026-46085>
- <https://bdu.fstec.ru/vul/2026-15654>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46198
BDU:2026-15674

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

Уязвимый продукт: Linux: от 6.19 до 7.0.8 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

98 **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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46198>
- <https://git.kernel.org/stable/c/f61499359fa529f0d45a53bf7c573a49eb6322e6>
- <https://git.kernel.org/stable/c/974542d1efc48b7e9fe16184e647615cba39969b>
- <https://git.kernel.org/stable/c/bf872db54f91ffe70104b98c20068b2d5910e018>
- <https://git.kernel.org/stable/c/b252797bfced986d6d92ec2f4cfcca842ce8aa78>
- <https://git.kernel.org/linus/0799e5943611006b346b8813c7daf7dd5aa26bfd>
- <https://security-tracker.debian.org/tracker/CVE-2026-46198>
- <https://ubuntu.com/security/CVE-2026-46198>
- <https://bdu.fstec.ru/vul/2026-15674>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46125
BDU:2026-15662

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.0 до 6.6.139 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46125>
- <https://git.kernel.org/stable/c/fe75fa1ac9a92990f7fc3d34b17808fd933071b2>
- <https://git.kernel.org/stable/c/afcbad89cdc1a001b43270cbf5394bb4804270a>
- <https://git.kernel.org/stable/c/9e28654f79f443bca9b29ff3ae7cf18abfba58a0>
- <https://git.kernel.org/stable/c/1c2b72ea89882aeb948340498391e69c58d466f1>
- <https://git.kernel.org/linus/283fc9e44ff5b5ac967439b4951b80bd4299f4e4>
- <https://security-tracker.debian.org/tracker/CVE-2026-46125>
- <https://ubuntu.com/security/CVE-2026-46125>

- <https://access.redhat.com/security/cve/CVE-2026-46125>
- <https://bdu.fstec.ru/vul/2026-15662>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46212
BDU:2026-15676

Идентификатор программной ошибки: CWE-364 Состояние гонки, связанное с обработчиком сигналов

Уязвимый продукт: Linux: от 3.5 до 5.10.257 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

100 **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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46212>
- <https://git.kernel.org/stable/c/368449e467d5f1e2c2e987bf2bd57000ba75e10b>
- <https://git.kernel.org/stable/c/6c5dc6d68e6ba7f0224a757a39ed52fcd54d472>
- <https://git.kernel.org/stable/c/00155f336a5e8b1006d2ca9ae7ad8fc4a44bb401>
- <https://git.kernel.org/stable/c/0cc9847c64cb6e61118bc78c9187c8209a7197fa>
- <https://git.kernel.org/linus/4ae1709a314060a196981b344610d023ea841e57>
- <https://security-tracker.debian.org/tracker/CVE-2026-46212>
- <https://ubuntu.com/security/CVE-2026-46212>
- <https://bdu.fstec.ru/vul/2026-15676>

101

Краткое описание: Выполнение произвольного кода в Crosswork Data Gateway

Идентификатор уязвимости: CVE-2026-20357
BDU:2026-15698

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

Уязвимый продукт: Cisco Crosswork Network Controller: до 7.2.1-SP
Crosswork Data Gateway: до 7.2.1-SP
Crosswork Planning: до 7.2.1-SP
Crosswork Workflow Manager: до 2.1.1-SP

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-crosswork-UzDTU9Vh>
- <https://bdu.fstec.ru/vul/2026-15698>

102

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46229
BDU:2026-15682

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

Уязвимый продукт: Linux: от 5.4 до 6.6.139 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46229>
- <https://git.kernel.org/stable/c/1db431380879fd9d28b763a88a0c0431be5be8df>
- <https://git.kernel.org/stable/c/32b153658f017ad2f5bf8aab479e8d16ac95bc3a>
- <https://git.kernel.org/stable/c/77d0b5d11387071770246fd0185a69fa28e8e109>
- <https://git.kernel.org/stable/c/047d44d8d29a6a1a5757256837aa9dd78e3cd0b5>
- <https://git.kernel.org/linus/ad52d61d82181dbdb7f05826de38352d5e550cc2>
- <https://security-tracker.debian.org/tracker/CVE-2026-46229>

- <https://ubuntu.com/security/CVE-2026-46229>
- <https://access.redhat.com/security/cve/CVE-2026-46229>
- <https://bdu.fstec.ru/vul/2026-15682>

103

Краткое описание: Выполнение произвольного кода в Microsoft QUIC

Идентификатор уязвимости: CVE-2026-62815
BDU:2026-15701

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 11 23H2: до 10.0.22631.7517
Windows 11 24H2: до 10.0.26100.9106
Windows Server 2022: до 10.0.20348.5440
Windows Server 2022 (Server Core installation): до 10.0.20348.5440
Windows Server 2025: до 10.0.26100.33222
Windows Server 2025 (Server Core installation): до 10.0.26100.33222
Windows 11 25H2: до 10.0.26200.9106
Windows 11 26H1: до 10.0.28000.2704

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-62815>
- <https://bdu.fstec.ru/vul/2026-15701>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46227
BDU:2026-15680

Идентификатор программной ошибки: CWE-188 Некорректные предположения о схеме организации данных или памяти

Уязвимый продукт: Linux: от 4.17 до 5.10.257 включительно
Red Hat Enterprise Linux: 9.4 Update Services for SAP Solutions
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46227>
- <https://git.kernel.org/stable/c/1bfb06ecb00f7fdf35dba8e8f2877346cbe5e078>
- <https://git.kernel.org/stable/c/6187a172d6ed57d6b2c327836e4407c6456e639d>
- <https://git.kernel.org/stable/c/c9dadb31f36045a8cb65df4bd75e7237ef21a4b5>
- <https://git.kernel.org/stable/c/bf0f40d8107e2ce827521968dc6926f3e13728ae>
- <https://git.kernel.org/linus/abb5f36771cc4c05899b34000829a787572a8817>
- <https://security-tracker.debian.org/tracker/CVE-2026-46227>
- <https://ubuntu.com/security/CVE-2026-46227>

- <https://access.redhat.com/security/cve/CVE-2026-46227>
- <https://bdu.fstec.ru/vul/2026-15680>

105

Краткое описание: Выполнение произвольного кода в Cisco Secure Workload

Идентификатор уязвимости: CVE-2026-20318
BDU:2026-15700

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Cisco Secure Workload: от 4.0 до 4.0.4.16

Категория уязвимого продукта: Средства защиты информации

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-csw1-shSvndWP>
- <https://bdu.fstec.ru/vul/2026-15700>

106

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46058
BDU:2026-15653

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

Уязвимый продукт: Linux: от 5.18 до 6.1.174 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46058>
- <https://git.kernel.org/stable/c/42dc622776f3ce1a6c31b13bdc686f7295e3b323>
- <https://git.kernel.org/stable/c/da4f46c5cf1d26e6b09418ad453e152f2e75a02c>
- <https://git.kernel.org/stable/c/fdc150dac1adb9a98be9d6956cff0348838b024a>
- <https://git.kernel.org/stable/c/6be2cb75bc1300080cfc8051579f22efae9401f7>
- <https://git.kernel.org/linus/8cd35ceadcfc8c5da2eb7f7ce24525ce9d4ee62e>
- <https://security-tracker.debian.org/tracker/CVE-2026-46058>
- <https://ubuntu.com/security/CVE-2026-46058>

- <https://bdu.fstec.ru/vul/2026-15653>

107

Краткое описание: Выполнение произвольного кода в Cisco Crosswork Data Gateway

Идентификатор уязвимости: CVE-2026-20358
BDU:2026-15697

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

Уязвимый продукт: Cisco Crosswork Network Controller: до 7.2.1-SP
Crosswork Data Gateway: до 7.2.1-SP
Crosswork Planning: до 7.2.1-SP
Crosswork Workflow Manager: до 2.1.1-SP

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-crosswork-UzDTU9Vh>
- <https://bdu.fstec.ru/vul/2026-15697>

108

Краткое описание: Выполнение произвольного кода в Cisco Crosswork Data Gateway

Идентификатор уязвимости: CVE-2026-20359
BDU:2026-15696

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

Уязвимый продукт: Cisco Crosswork Network Controller: до 7.2.1-SP
Crosswork Data Gateway: до 7.2.1-SP
Crosswork Planning: до 7.2.1-SP
Crosswork Workflow Manager: до 2.1.1-SP

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.9 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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-crosswork-UzDTU9Vh>
- <https://bdu.fstec.ru/vul/2026-15696>

109

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46240
BDU:2026-15687

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.19.6 до 7.0.8 включительно
Ubuntu: 26.04 LTS

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46240>
- <https://git.kernel.org/stable/c/dd24998a4a4016fb9921916024399bd80f0d45c6>
- <https://git.kernel.org/stable/c/18c64439f249859b6140f7bf8bcf95c8ed841f28>
- <https://git.kernel.org/linus/f27cfdcfc916bb59297825805f4c3499f89f9e76>
- <https://ubuntu.com/security/CVE-2026-46240>
- <https://bdu.fstec.ru/vul/2026-15687>

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46232
BDU:2026-15684

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

Уязвимый продукт: Linux: от 6.19 до 7.0.8 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46232>
- <https://git.kernel.org/stable/c/0bc4cf1a6ba00fb8c074531b179bc7b97502fbc4>
- <https://git.kernel.org/stable/c/9c031b24aed6733b6dcc5d98527875b8654a04e9>
- <https://git.kernel.org/stable/c/7812694752a5f295eaa05a093b90a2c332666051>
- <https://git.kernel.org/stable/c/208f6d5b1dfd6399bc6af9e11f27f1f496243ed0>
- <https://git.kernel.org/linus/cac61b58a3b6340c52afa06bb15eac033158db2f>
- <https://security-tracker.debian.org/tracker/CVE-2026-46232>
- <https://ubuntu.com/security/CVE-2026-46232>
- <https://bdu.fstec.ru/vul/2026-15684>

111

Краткое описание: Выполнение произвольного кода в Cisco Crosswork Data Gateway

Идентификатор уязвимости: CVE-2026-20030
BDU:2026-15699

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

Уязвимый продукт: Cisco Crosswork Network Controller: до 7.2.1-SP
Crosswork Data Gateway: до 7.2.1-SP
Crosswork Planning: до 7.2.1-SP
Crosswork Workflow Manager: до 2.1.1-SP

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-crosswork-UzDTU9Vh>
- <https://bdu.fstec.ru/vul/2026-15699>

112

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46037
BDU:2026-15651

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Linux: от 6.7 до 6.12.85 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Red Hat OpenShift Container Platform: 4.16

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46037>
- <https://git.kernel.org/stable/c/92e7c209036dcc0e8ffdf806fd3645b263bea5>
- <https://git.kernel.org/stable/c/bc64a66e0b9ad937d3d49934242ee62b01ba9a94>
- <https://git.kernel.org/stable/c/c2178ff1c70ebfc2ab9651b230c58a34683db759>
- <https://git.kernel.org/stable/c/d700c34a5d186b9ba0715bcb19e0ff80ffbfbfc1>
- <https://git.kernel.org/linus/67bf002a2d7387a6312138210d0bd06e3cf4879b>
- <https://security-tracker.debian.org/tracker/CVE-2026-46037>

- <https://ubuntu.com/security/CVE-2026-46037>
- <https://access.redhat.com/security/cve/CVE-2026-46037>
- <https://bdu.fstec.ru/vul/2026-15651>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-45989
BDU:2026-15636

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.6 до 6.6.139 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

113 **Оценка CVSSv3:** 8.0 AV:A/AC:L/PR:L/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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-45989>
- <https://git.kernel.org/stable/c/0ba03e06f037df704d9b032e36d417633e2326bc>
- <https://git.kernel.org/stable/c/d68347b07b9801791c9eaab8f772770b52b8cd5c>
- <https://git.kernel.org/stable/c/5b6122a67a295f8a08b7c18d908a1bd974dfaec8>
- <https://git.kernel.org/stable/c/6b2023286d2c6ed3bf964fb92e34c9c14d42eb69>
- <https://git.kernel.org/linus/07fd339b2c253205794bea5d9b4b7548a4546c56>
- <https://security-tracker.debian.org/tracker/CVE-2026-45989>
- <https://ubuntu.com/security/CVE-2026-45989>
- <https://bdu.fstec.ru/vul/2026-15636>

114

Краткое описание: Чтение локальных файлов в Grafana MCP Server

Идентификатор уязвимости: CVE-2026-19516
BDU:2026-15573

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

Уязвимый продукт: Grafana MCP Server: до 1.1.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Чтение локальных файлов

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://github.com/HORKimhab/CVE-2026-19516>
- <https://grafana.com/security/security-advisories/cve-2026-19516/>
- <https://www.sentinelone.com/vulnerability-database/cve-2026-19516/>
- <https://bdu.fstec.ru/vul/2026-15573>

115

Краткое описание: Выполнение произвольного кода в Swiper

Идентификатор уязвимости: CVE-2026-27212
BDU:2026-15574

Идентификатор программной ошибки: CWE-1008 Архитектурные принципы

Уязвимый продукт: Swiper: от 6.5.1 до 12.1.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://github.com/nolimits4web/swiper/commit/d3e663322a13043ca63aaba235d8cf3900e0c8cf>
- <https://github.com/nolimits4web/swiper/releases/tag/v12.1.2>
- <https://github.com/nolimits4web/swiper/security/advisories/GHSA-hmx5-qpq5-p643>
- <https://bdu.fstec.ru/vul/2026-15574>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-89775
BDU:2026-15576

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

Уязвимый продукт: Linux: до 7.3-rc1
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Amazon Linux: 2023

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://lore.kernel.org/linux-cve-announce/2026091628-CVE-2026-89775-7caf@gregkh/>
- <https://git.kernel.org/stable/c/be54a70067c7dbe1381157e8a238fa4b16ea9c05>
- <https://git.kernel.org/stable/c/1c9fca34b9625a67a7f1a03c8604f3df760c6c49>
- <https://git.kernel.org/stable/c/8053393680d4fa3eb962667d2be95dd39f0940e5>
- <https://www.opennet.ru/opennews/art.shtml?num=66310>
- <https://access.redhat.com/security/cve/cve-2026-89775>
- <https://explore.alas.aws.amazon.com/CVE-2026-89775.html>
- <https://feedly.com/cve/CVE-2026-89775>

- <https://ubuntu.com/security/cve-2026-89775>
- <https://bdu.fstec.ru/vul/2026-15576>

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

Идентификатор уязвимости: CVE-2026-72972
BDU:2026-15583

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

Уязвимый продукт: Microsoft 365 Apps for Enterprise: до 16.0.20326.20138
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Office LTSC 2024: до 16.0.17932.20976
Microsoft Office 2019: до 16.0.10417.20207
Microsoft Word 2016: до 16.0.5569.1000
Microsoft Office 365: до 16.113.26091433

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

117 **Последствия эксплуатации:** Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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:N/A:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72972>
- <https://bdu.fstec.ru/vul/2026-15583>

Краткое описание: Повышение привилегий в Windows Network Connection Broker

Идентификатор уязвимости: CVE-2026-72967
BDU:2026-15584

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

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23398
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23398
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72967>
- <https://bdu.fstec.ru/vul/2026-15584>

Краткое описание: Повышение привилегий в Windows WebClient Service

Идентификатор уязвимости: CVE-2026-72965
BDU:2026-15585

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows 10 1607: до 10.0.14393.9512
Windows 10 1809: до 10.0.17763.9245
Windows 10 21H2: до 10.0.19044.7725
Windows 10 22H2: до 10.0.19045.7725
Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
Windows Server 2012: до 6.2.9200.26349
Windows Server 2012 R2: до 6.3.9600.23398
Windows Server 2012 (Server Core installation): до 6.2.9200.26349
Windows Server 2012 R2 (Server Core installation): до 6.3.9600.23398
Windows Server 2016: до 10.0.14393.9512
Windows Server 2016 (Server Core installation): до 10.0.14393.9512
Windows Server 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
Windows Server 2022: до 10.0.20348.5622
Windows Server 2022 (Server Core installation): до 10.0.20348.5622
Windows Server 2025: до 10.0.26100.33438
Windows Server 2025 (Server Core installation): до 10.0.26100.33438
Windows 11 25H2: до 10.0.26200.9445
Windows 11 26H1: до 10.0.28000.2954

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: 2026-09-29 / 2026-09-29

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72965>
- <https://bdu.fstec.ru/vul/2026-15585>

120

Краткое описание: Повышение привилегий в Microsoft Entra ID

Идентификатор уязвимости: CVE-2026-69851
BDU:2026-15589

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

Уязвимый продукт: Microsoft Entra ID: -

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 9.9 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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-69851>
- <https://bdu.fstec.ru/vul/2026-15589>

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46024
BDU:2026-15644

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Linux: от 2.6.34 до 5.15.208 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 7.5 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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46024>
- <https://git.kernel.org/stable/c/4b2738b93edad661178340239de657d876b73d3d>
- <https://git.kernel.org/stable/c/927e4bd5692f2a4901808822981fb2c8d4456548>
- <https://git.kernel.org/stable/c/016bc663657366d386993f63eb31072eb45a2b77>
- <https://git.kernel.org/stable/c/8f2be7285941a33a9f72579a23b96392f83c758e>
- <https://git.kernel.org/linus/5199c125d25aeae8615c4fc31652cc0fe624338e>
- <https://security-tracker.debian.org/tracker/CVE-2026-46024>
- <https://ubuntu.com/security/CVE-2026-46024>

- <https://access.redhat.com/security/cve/CVE-2026-46024>
- <https://bdu.fstec.ru/vul/2026-15644>

122

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46015
BDU:2026-15642

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

Уязвимый продукт: Linux: от 5.14 до 5.15.208 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46015>
- <https://git.kernel.org/stable/c/ab5fdcd535645f6dbe6e9e21d96a08d141e88b4b>
- <https://git.kernel.org/stable/c/bebd058ef40c67a81fe6d9ee8beaa4ede90e0704>
- <https://git.kernel.org/stable/c/83bb57635d7cbafde32f865b577ecfd969f02337>
- <https://git.kernel.org/stable/c/12625b4da84caf4d84a04988710a7b9bcf702b18>
- <https://git.kernel.org/linus/3864c6ba1e041bc75342353a70fa2a2c6f909923>
- <https://security-tracker.debian.org/tracker/CVE-2026-46015>

- <https://ubuntu.com/security/CVE-2026-46015>
- <https://access.redhat.com/security/cve/CVE-2026-46015>
- <https://bdu.fstec.ru/vul/2026-15642>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46011
BDU:2026-15640

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Linux: от 6.7 до 6.12.85 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

123 **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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46011>
- <https://git.kernel.org/stable/c/2209fdae5c2f615930c9af1379c1cfca199ec5d8>
- <https://git.kernel.org/stable/c/0498b27a1542021d90269d58347501d4c3ccd84e>
- <https://git.kernel.org/stable/c/26506a30e0e26d612f82a7bf0e395626968a44e6>
- <https://git.kernel.org/stable/c/e78c39f720679fcf3a2eacd82725ec3ea2648301>
- <https://git.kernel.org/linus/34c519feef3e4fcff1078dc8bdb25fbbbd10303f>
- <https://security-tracker.debian.org/tracker/CVE-2026-46011>
- <https://ubuntu.com/security/CVE-2026-46011>
- <https://bdu.fstec.ru/vul/2026-15640>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46010
BDU:2026-15639

Идентификатор программной ошибки: CWE-253 Некорректная проверка значений, возвращаемых функцией

Уязвимый продукт: Linux: от 6.16.9 до 6.18.26 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.1 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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46010>
- <https://git.kernel.org/stable/c/293095ef618818852bac5488c1bc223935e2ca17>
- <https://git.kernel.org/stable/c/c52803e925604e2a17962ab0c99dce2d3f7238db>
- <https://git.kernel.org/linus/3476c8bb960f48e49355d6f93fb7673211e0163f>
- <https://ubuntu.com/security/CVE-2026-46010>
- <https://access.redhat.com/security/cve/CVE-2026-46010>
- <https://bdu.fstec.ru/vul/2026-15639>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46006
BDU:2026-15638

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

Уязвимый продукт: Linux: от 2.6.34 до 5.15.208 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

125 **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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46006>
- <https://git.kernel.org/stable/c/fa297e919d1680c38ab268ff952b1698dac987f6>
- <https://git.kernel.org/stable/c/d749a9a0ee4014681487e7ae549901aa8c176637>
- <https://git.kernel.org/stable/c/332884f5eb79dd60a7162b079d09d39208567a31>
- <https://git.kernel.org/stable/c/e441d5c23ec644c8d27593db3b8928e8933512a9>
- <https://git.kernel.org/linus/2fc87d37be1b730a149b035f9375fdb8cc5333a5>
- <https://security-tracker.debian.org/tracker/CVE-2026-46006>
- <https://ubuntu.com/security/CVE-2026-46006>
- <https://bdu.fstec.ru/vul/2026-15638>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-46001
BDU:2026-15637

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Linux: от 6.9 до 6.12.85 включительно
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

126

Оценка CVSSv3: 8.0 AV:A/AC:L/PR:L/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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46001>
- <https://git.kernel.org/stable/c/7eccabff1c9ec15e4b6fe186d5c147b13a9cdb4e>
- <https://git.kernel.org/stable/c/95d48e37a1304d6148406c799479c0fb505aefa7>
- <https://git.kernel.org/stable/c/a11aa9c5fd9dfe62be7cfec1f2a7546afb77254c>
- <https://git.kernel.org/linus/24c73e93d6a756e1b8626bb259d2e07c5b89b370>
- <https://security-tracker.debian.org/tracker/CVE-2026-46001>
- <https://ubuntu.com/security/CVE-2026-46001>
- <https://bdu.fstec.ru/vul/2026-15637>

Краткое описание: Отказ в обслуживании в Linux

Идентификатор уязвимости: CVE-2026-46027
BDU:2026-15646

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Linux: от 4.11 до 5.10.257 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13

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

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Отказ в обслуживании

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

Оценка CVSSv3: 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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-46027>
- <https://git.kernel.org/stable/c/f0858e1d5624bb120b198f2a8528f97a9b0ae069>
- <https://git.kernel.org/stable/c/6180a296ca65b08a81914805cbc0f78da5f10a1f>
- <https://git.kernel.org/stable/c/ea0b5d0fe96356dce38f98375a57c52a04e13712>
- <https://git.kernel.org/stable/c/83bcf9228b0501694fb2589ed1d142855a2887f2>
- <https://git.kernel.org/linus/5a8db80f721deee8e916c2cfdee78decda02ce4f>
- <https://security-tracker.debian.org/tracker/CVE-2026-46027>
- <https://ubuntu.com/security/CVE-2026-46027>

- <https://access.redhat.com/security/cve/CVE-2026-46027>
- <https://bdu.fstec.ru/vul/2026-15646>

128

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-45959
BDU:2026-15634

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

Уязвимый продукт: Linux: от 6.17 до 6.18.13 включительно
Red Hat Enterprise Linux: 10
Ubuntu: 24.04 LTS

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-45959>
- <https://git.kernel.org/stable/c/9a3ace9b010ffd8c422c97844ae152f7c53d6b18>
- <https://git.kernel.org/stable/c/90f9090e3e744a8fe3bb6fa0e61f577347728b0b>
- <https://git.kernel.org/linus/d5abcc33ee76bc26d58b39dc1a097e43a99dd438>
- <https://ubuntu.com/security/CVE-2026-45959>
- <https://access.redhat.com/security/cve/CVE-2026-45959>
- <https://bdu.fstec.ru/vul/2026-15634>

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-43493
BDU:2026-15627

Идентификатор программной ошибки: CWE-310 Уязвимости, связанные с криптографией

Уязвимый продукт: Linux: от 6.19 до 7.0.3 включительно
Debian GNU/Linux: 13

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

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Выполнение произвольного кода

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

129 **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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://www.cve.org/CVERecord?id=CVE-2026-43493>
- <https://git.kernel.org/stable/c/9f1cbca178c03188e201ed175251372149bb25f2>
- <https://git.kernel.org/stable/c/eb34e243df57e32f4c08fa191f3602ea19076276>
- <https://git.kernel.org/stable/c/77d55bc8675ee851ed639dc9be77325a8024cf67>
- <https://git.kernel.org/stable/c/46271895ddfb1ba41f89f7e0dffbe9c2bcf7380a>
- <https://git.kernel.org/linus/915b692e6cb723aac658c25eb82c58fd81235110>
- <https://security-tracker.debian.org/tracker/CVE-2026-43493>
- <https://bdu.fstec.ru/vul/2026-15627>

130

Краткое описание: Повышение привилегий в Microsoft Exchange Online

Идентификатор уязвимости: CVE-2026-65801
BDU:2026-15596

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

Уязвимый продукт: Microsoft Exchange Server: -

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65801>
- <https://bdu.fstec.ru/vul/2026-15596>

131

Краткое описание: Повышение привилегий в Microsoft Fabric

Идентификатор уязвимости: CVE-2026-63509
BDU:2026-15631

Идентификатор программной ошибки: CWE-23 Подмена относительного пути

Уязвимый продукт: Microsoft Fabric: -

Категория уязвимого продукта: Серверное программное обеспечение и его 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: 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: 2026-09-30 / 2026-09-30

Ссылки на источник:

- <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-63509>
- <https://bdu.fstec.ru/vul/2026-15631>