НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-11-18.1 | 18 ноября 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2026-109619	PHP	Сетевой	ACE	2026-10-21	✓
2	Критическая	CVE-2026-109618	PHP	Сетевой	ACE	2026-10-21	✓
3	Критическая	CVE-2026-110264	Gitlab	Сетевой	ACE	2026-10-23	✓
4	Высокая	CVE-2026-56736	phpMyFAQ	Сетевой	XSS\CSS	2026-09-30	✓
5	Высокая	CVE-2026-56737	phpMyFAQ	Сетевой	OSI	2026-09-30	✓
6	Высокая	CVE-2026-71540	Wazuh	Сетевой	DoS	2026-09-30	✓
7	Критическая	CVE-2026-100721	vm2	Сетевой	ACE	2026-09-30	✓
8	Высокая	CVE-2026-101903	axios	Сетевой	DoS	2026-10-01	✓
9	Высокая	CVE-2026-101905	axios	Сетевой	OSI	2026-10-01	✓
10	Высокая	CVE-2026-64508	Linux	Локальный	ACE	2026-10-01	✓
11	Высокая	CVE-2026-101898	axios	Сетевой	SB	2026-10-01	✓
12	Высокая	CVE-2026-101901	axios	Сетевой	DoS	2026-10-01	✓
13	Критическая	CVE-2026-101904	axios	Сетевой	SB	2026-10-01	✓

14	Критическая	CVE-2026-76504	Catalyst SD-WAN Manager	Сетевой	SB	2026-10-01	✓
15	Высокая	CVE-2026-95387	Wireshark	Сетевой	ACE	2026-10-01	✓
16	Высокая	CVE-2026-95389	Wireshark	Сетевой	ACE	2026-10-01	✓
17	Высокая	CVE-2026-101906	axios	Сетевой	DoS	2026-10-01	✓
18	Критическая	CVE-2026-102268	PyJWT	Сетевой	SB	2026-10-01	✓
19	Высокая	CVE-2026-55987	Gitea	Сетевой	CI	2026-10-02	✓
20	Высокая	CVE-2026-54481	Gitea	Смежная сеть	ACE	2026-10-02	✓
21	Критическая	CVE-2026-56443	Gitea	Сетевой	OAF	2026-10-02	✓
22	Высокая	CVE-2026-58314	Gitea	Сетевой	OSI	2026-10-01	✓
23	Высокая	CVE-2026-58417	Gitea	Сетевой	OSI	2026-10-01	✓
24	Критическая	CVE-2026-48273	ColdFusion	Сетевой	ACE	2026-10-02	✓
25	Высокая	CVE-2026-102990	basic-ftp	Сетевой	DoS	2026-10-02	✓
26	Высокая	CVE-2026-103111	PCRE2	Сетевой	OAF	2026-10-02	✓
27	Высокая	CVE-2026-102992	Piscina	Сетевой	ACE	2026-10-02	✓
28	Критическая	CVE-2026-104286	FortiMail	Сетевой	ACE	2026-10-02	✓

29	Высокая	CVE-2026-58427	РЕД ОС	Сетевой	OSI	2026-10-01	✓
30	Высокая	CVE-2026-83970	Windows Biometric Service	Локальный	PE	2026-10-05	✓
31	Высокая	CVE-2026-83969	Windows Biometric Service	Локальный	PE	2026-10-05	✓
32	Высокая	CVE-2026-83967	Windows Biometric Service	Локальный	PE	2026-10-05	✓
33	Высокая	CVE-2026-83955	Windows Biometric Service	Локальный	PE	2026-10-05	✓
34	Высокая	CVE-2026-83971	Windows Biometric Service	Локальный	PE	2026-10-05	✓
35	Критическая	CVE-2026-41252	xrdp	Сетевой	ACE	2026-10-02	✓
36	Высокая	CVE-2026-83974	Windows Biometric Service	Локальный	PE	2026-10-05	✓
37	Высокая	CVE-2026-83976	Windows Biometric Service	Локальный	PE	2026-10-05	✓
38	Высокая	CVE-2026-83977	Windows Biometric Service	Локальный	PE	2026-10-05	✓
39	Высокая	CVE-2026-83978	Windows Biometric Service	Локальный	PE	2026-10-05	✓
40	Высокая	CVE-2026-83972	Windows Biometric Service	Локальный	PE	2026-10-05	✓
41	Высокая	CVE-2026-83980	Windows Biometric Service	Локальный	PE	2026-10-05	✓
42	Высокая	CVE-2026-88779	NetScaler Gateway	Сетевой	DoS	2026-10-05	✓
43	Критическая	CVE-2026-102829	simple-git	Сетевой	SB	2026-10-02	✓

44	Высокая	CVE-2026-83981	Windows Biometric Service	Локальный	PE	2026-10-05	✓
45	Высокая	CVE-2026-83983	Windows Biometric Service	Локальный	PE	2026-10-05	✓
46	Высокая	CVE-2026-83982	Windows Biometric Service	Локальный	PE	2026-10-05	✓
47	Высокая	CVE-2026-83975	Windows Biometric Service	Локальный	PE	2026-10-05	✓
48	Высокая	CVE-2026-83973	Windows Biometric Service	Локальный	PE	2026-10-05	✓
49	Высокая	CVE-2026-103263	Tornado	Сетевой	RLF	2026-10-05	✓
50	Высокая	CVE-2026-83968	Windows Biometric Service	Локальный	PE	2026-10-05	✓
51	Высокая	CVE-2026-83979	Windows Biometric Service	Локальный	PE	2026-10-05	✓
52	Высокая	CVE-2026-83985	Windows Biometric Service	Локальный	PE	2026-10-05	✓
53	Высокая	CVE-2026-81379	Visual Studio Code	Сетевой	SB	2026-10-06	✓
54	Высокая	CVE-2026-83498	Windows Virtualization-Based Security Enclave	Локальный	PE	2026-10-06	✓
55	Высокая	CVE-2026-83939	Windows Secure Kernel Mode	Локальный	PE	2026-10-06	✓
56	Высокая	CVE-2026-83942	Windows Kernel	Локальный	PE	2026-10-06	✓
57	Высокая	CVE-2026-81354	Windows Hello	Локальный	PE	2026-10-06	✓
58	Высокая	CVE-2026-80096	Windows Remote Desktop Services	Сетевой	PE	2026-10-06	✓

59	Высокая	CVE-2026-81355	Virtual Hard Disk Miniport Driver	Локальный	ACE	2026-10-06	✓
60	Высокая	CVE-2026-80083	Windows Hyper-V	Локальный	ACE	2026-10-06	✓
61	Высокая	CVE-2026-81378	Visual Studio Code	Сетевой	SB	2026-10-06	✓
62	Высокая	CVE-2026-83952	Windows Resilient File System	Локальный	PE	2026-10-06	✓
63	Высокая	CVE-2026-81357	Visual Studio Code	Сетевой	SB	2026-10-06	✓
64	Высокая	CVE-2026-77120	PowerLogic T300	Локальный	PE	2026-09-17	✓
65	Высокая	CVE-2026-83954	Windows Biometric Service	Локальный	PE	2026-10-06	✓
66	Высокая	CVE-2026-81356	Visual Studio Code	Сетевой	SB	2026-10-06	✓
67	Критическая	BDU:2026-15971	Libheif	Сетевой	ACE	2026-10-06	✓
68	Высокая	CVE-2026-72959	Windows Routing and Remote Access Service	Сетевой	ACE	2026-09-29	✓
69	Высокая	CVE-2026-72960	Windows Media Player	Сетевой	ACE	2026-09-29	✓
70	Высокая	CVE-2026-72961	Windows Hyper-V	Локальный	PE	2026-09-29	✓
71	Критическая	CVE-2026-42322	piwigo	Сетевой	ACE	2026-10-06	✓
72	Высокая	CVE-2026-64074	Linux	Локальный	ACE	2026-08-05	✓
73	Критическая	CVE-2026-12569	PTC Windchill PDMLink и PTC FlexPLM	Сетевой	ACE	2026-10-06	✓

74	Высокая	CVE-2026-72962	Windows USB Video Driver	Локальный	PE	2026-09-29	✓
75	Высокая	CVE-2026-80075	Windows Work Folders	Локальный	PE	2026-10-07	✓
76	Высокая	CVE-2026-78444	Microsoft Failover Cluster	Сетевой	ACE	2026-10-07	✓
77	Высокая	CVE-2026-78442	Windows OLE DB	Сетевой	ACE	2026-10-07	✓
78	Высокая	CVE-2026-78439	Microsoft Office Graphics Component	Сетевой	ACE	2026-10-07	✓
79	Высокая	CVE-2026-77909	Azure CycleCloud	Сетевой	OSI	2026-10-07	✓
80	Высокая	CVE-2026-77908	Microsoft Dynamics 365 On-Premises	Сетевой	ACE	2026-10-07	✓
81	Высокая	CVE-2026-77907	Visual Studio	Сетевой	ACE	2026-10-07	✓
82	Высокая	CVE-2026-77906	Visual Studio	Сетевой	ACE	2026-10-07	✓
83	Высокая	CVE-2026-80077	Windows Remote Desktop Client	Сетевой	ACE	2026-10-07	✓
84	Высокая	CVE-2026-80074	Windows Remote Desktop Client	Сетевой	ACE	2026-10-07	✓
85	Высокая	CVE-2026-21589	Atlassian Data Center	Сетевой	OSI	2026-10-07	✓
86	Высокая	CVE-2026-78505	Microsoft Office	Сетевой	ACE	2026-10-07	✓
87	Высокая	CVE-2026-16444	TeamViewer	Сетевой	ACE	2026-10-07	✓
88	Высокая	CVE-2026-78504	Microsoft Office Word	Сетевой	ACE	2026-10-07	✓

89	Высокая	CVE-2026-78512	Microsoft Office Word	Сетевой	ACE	2026-10-07	✓
90	Высокая	CVE-2026-78517	Microsoft Office Word	Сетевой	ACE	2026-10-07	✓
91	Высокая	CVE-2026-78518	Microsoft Office Excel	Сетевой	ACE	2026-10-07	✓
92	Высокая	CVE-2026-78511	Microsoft Office Word	Сетевой	ACE	2026-10-07	✓
93	Высокая	CVE-2026-78519	Microsoft Office Outlook	Сетевой	ACE	2026-10-07	✓
94	Высокая	CVE-2026-78507	Microsoft Office Word	Сетевой	ACE	2026-10-07	✓
95	Высокая	CVE-2026-78514	Microsoft Office Word	Сетевой	ACE	2026-10-07	✓
96	Высокая	CVE-2026-78521	Microsoft Office Word	Сетевой	ACE	2026-10-07	✓
97	Высокая	CVE-2026-77489	Windows Biometric Service	Локальный	PE	2026-10-08	✓
98	Высокая	CVE-2026-77494	Windows DHCP Server	Сетевой	DoS	2026-10-08	✓
99	Высокая	CVE-2026-77498	Windows DHCP Server	Сетевой	DoS	2026-10-08	✓
100	Высокая	CVE-2026-77495	Windows Imaging Component	Сетевой	ACE	2026-10-08	✓
101	Высокая	CVE-2026-78450	Windows Reliable Multicast Transport Driver	Сетевой	ACE	2026-10-07	✓
102	Высокая	CVE-2026-78449	Windows Reliable Multicast Transport Driver	Сетевой	ACE	2026-10-07	✓
103	Высокая	CVE-2026-107213	excelize	Сетевой	DoS	2026-10-08	✓

104	Высокая	CVE-2026-77487	SQL Server	Сетевой	PE	2026-10-08	✓
105	Высокая	CVE-2026-73011	Windows Biometric Service	Локальный	PE	2026-10-07	✓
106	Высокая	CVE-2026-77483	SQL Server	Сетевой	PE	2026-10-08	✓
107	Высокая	CVE-2026-77480	SQL Server	Сетевой	PE	2026-10-08	✓
108	Высокая	CVE-2026-73028	SQL Server	Сетевой	PE	2026-10-08	✓
109	Высокая	CVE-2026-73007	Windows Biometric Service	Локальный	PE	2026-10-07	✓
110	Высокая	CVE-2026-73015	Windows Biometric Service	Локальный	PE	2026-10-07	✓
111	Высокая	CVE-2026-73020	Windows Biometric Service	Локальный	PE	2026-10-07	✓
112	Высокая	CVE-2026-73021	Windows Biometric Service	Локальный	PE	2026-10-07	✓
113	Высокая	CVE-2026-73026	Windows Biometric Service	Локальный	PE	2026-10-07	✓
114	Высокая	CVE-2026-78456	SQL Server	Сетевой	ACE	2026-10-07	✓
115	Высокая	CVE-2026-77484	Microsoft SQL Server	Сетевой	ACE	2026-10-08	✓
116	Высокая	CVE-2026-78463	Windows Remote Desktop Client	Сетевой	ACE	2026-10-07	✓
117	Высокая	CVE-2026-77901	Microsoft Office Word	Сетевой	ACE	2026-10-08	✓
118	Высокая	CVE-2026-78447	Windows Biometric Service	Локальный	PE	2026-10-07	✓

119	Высокая	CVE-2026-78462	Visual Studio Code	Сетевой	SB	2026-10-07	✓
120	Критическая	CVE-2026-57967	Apache ActiveMQ Artemis и Apache Artemis	Сетевой	ACE	2026-10-07	✓
121	Высокая	CVE-2026-102422	shell-quote	Сетевой	ACE	2026-10-08	✓
122	Высокая	CVE-2026-77500	Windows Device Association Service	Локальный	PE	2026-10-08	✓
123	Высокая	CVE-2026-77502	Windows DHCP Server	Сетевой	DoS	2026-10-08	✓
124	Высокая	CVE-2026-77886	Windows DHCP Server	Сетевой	DoS	2026-10-08	✓
125	Высокая	CVE-2026-77893	Windows DHCP Server	Сетевой	DoS	2026-10-08	✓
126	Высокая	CVE-2026-77895	Windows DHCP Server	Сетевой	DoS	2026-10-08	✓
127	Высокая	CVE-2026-77501	Windows DHCP Server	Сетевой	DoS	2026-10-08	✓
128	Высокая	CVE-2026-77889	Windows DHCP Server	Сетевой	DoS	2026-10-08	✓
129	Высокая	CVE-2026-77888	Windows DHCP Server	Сетевой	DoS	2026-10-08	✓
130	Высокая	CVE-2026-77505	Windows DNS Server	Сетевой	ACE	2026-10-08	✓
131	Высокая	CVE-2026-77503	Windows NTFS	Локальный	PE	2026-10-08	✓
132	Высокая	CVE-2026-77504	Microsoft Office Word	Сетевой	ACE	2026-10-08	✓
133	Высокая	CVE-2026-77904	Windows Volume Manager Extension Driver	Локальный	PE	2026-10-08	✓

134	Высокая	CVE-2026-77898	Microsoft Office	Сетевой	ACE	2026-10-08	✓
135	Высокая	CVE-2026-77499	Windows DHCP Server	Сетевой	DoS	2026-10-08	✓
136	Высокая	CVE-2026-77890	Windows DHCP Server	Сетевой	DoS	2026-10-08	✓
137	Высокая	CVE-2026-78448	Windows Biometric Service	Локальный	PE	2026-10-07	✓
138	Высокая	CVE-2026-73014	Data Sharing Service Client	Локальный	PE	2026-10-08	✓
139	Высокая	CVE-2026-77486	Microsoft SQL Server	Сетевой	ACE	2026-10-07	✓
140	Высокая	CVE-2026-77482	Microsoft SQL Server	Сетевой	ACE	2026-10-07	✓
141	Высокая	CVE-2026-77481	Microsoft SQL Server	Сетевой	ACE	2026-10-07	✓
142	Высокая	CVE-2026-73023	Windows Imaging Component	Сетевой	ACE	2026-10-07	✓
143	Высокая	CVE-2026-73013	Windows Imaging Component	Сетевой	ACE	2026-10-07	✓
144	Высокая	CVE-2026-73012	Windows Management Services	Сетевой	PE	2026-10-07	✓
145	Критическая	CVE-2026-76500	Cisco APIC	Сетевой	ACE	2026-10-09	✓
146	Критическая	CVE-2026-76499	Cisco APIC	Сетевой	ACE	2026-10-09	✓
147	Критическая	CVE-2026-76498	Cisco APIC	Сетевой	ACE	2026-10-09	✓
148	Критическая	CVE-2026-76486	NX-OS	Сетевой	ACE	2026-10-09	✓

149	Критическая	CVE-2026-76485	NX-OS	Сетевой	ACE	2026-10-09	✓
150	Высокая	CVE-2026-76484	Cisco Smart Software Manager On-Prem	Сетевой	ACE	2026-10-09	✓
151	Критическая	CVE-2026-76480	Cisco Smart Software Manager On-Prem	Сетевой	ACE	2026-10-09	✓
152	Критическая	CVE-2026-76482	Cisco Smart Software Manager On-Prem	Сетевой	ACE	2026-10-09	✓
153	Критическая	CVE-2026-76483	Cisco Smart Software Manager On-Prem	Сетевой	OSI	2026-10-09	✓

1

Краткое описание: Выполнение произвольного кода в PHP

Идентификатор уязвимости: CVE-2026-109619
BDU:2026-17192

Идентификатор программной ошибки: CWE-1065 Компонент, созданный для работы на сервере, использует элементы управления ресурсами среды исполнения

Уязвимый продукт: PHP: от 8.5.0 до 8.5.12
Astra Linux Common Edition: 1.6 «Смоленск»
PAN-OS: 11.1
Astra Linux Special Edition: 4.8
PT NGFW: до 1.11.2 включительно (сертифицировано: 1.10.3)
Программный межсетевой экран Интернет Контроль Сервер (ФСТЭК): до 13.4.1 включительно
Panorama: -

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного POST-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:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-21 / 2026-10-21

Ссылки на источник:

- https://ptsecurity.com/research/threatscape/PT-2026-32/
- https://sansec.io/research/php2shell
- https://cert.europa.eu/publications/security-advisories/2026-018
- https://www.php.net/archive/2026.php#2026-10-20-1

- https://www.linux.org.ru/news/security/18405491
- https://github.com/php/php-src/releases#release-php-8.2.35
- https://github.com/php/php-src/releases#release-php-8.3.36
- https://github.com/php/php-src/releases#release-php-8.4.27
- https://github.com/php/php-src/releases#release-php-8.5.12
- https://security.paloaltonetworks.com/CVE-2026-109619
- https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp
- https://github.com/9bie/php2shell-bypass-aslr-exp
- https://github.com/xuehuolll/php2shell-CVE-2026-109618-109619/tree/63618bd7629dbfc2d5b505e9dd74e321d8345351
- https://php2shell.ru/
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://github.com/NeoArtemis37/PHP2shell
- https://wiki.astralinux.ru/x/jo0tI
- https://wiki.astralinux.ru/x/3YwtI
- https://wiki.astralinux.ru/x/no0tI
- https://wiki.astralinux.ru/x/lo0tI
- https://wiki.astralinux.ru/x/k40tI
- https://wiki.astralinux.ru/x/mI0tI
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-1102SE18HF
- https://wiki.astralinux.ru/astra-linux-se17-bulletin-2026-1109SE17HF
- https://bdu.fstec.ru/vul/2026-17192

2

Краткое описание: Выполнение произвольного кода в PHP

Идентификатор уязвимости: CVE-2026-109618
BDU:2026-17191

Идентификатор программной ошибки: CWE-1065 Компонент, созданный для работы на сервере, использует элементы управления ресурсами среды исполнения

Уязвимый продукт: PHP: от 8.5.0 до 8.5.12
Astra Linux Common Edition: 1.6 «Смоленск»
PAN-OS: 11.1
Astra Linux Special Edition: 4.8
Программный межсетевой экран Интернет Контроль Сервер: до 13.4.1 включительно
PT NGFW: до 1.11.2 включительно (сертифицировано: 1.10.3)
Panorama: -

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданного POST-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:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-21 / 2026-10-21

Ссылки на источник:

- https://ptsecurity.com/research/threatscape/PT-2026-31/
- https://sansec.io/research/php2shell
- https://cert.europa.eu/publications/security-advisories/2026-018
- https://www.php.net/archive/2026.php#2026-10-20-1

- https://www.linux.org.ru/news/security/18405491
- https://github.com/php/php-src/releases#release-php-8.2.35
- https://github.com/php/php-src/releases#release-php-8.3.36
- https://github.com/php/php-src/releases#release-php-8.4.27
- https://github.com/php/php-src/releases#release-php-8.5.12
- https://security.paloaltonetworks.com/CVE-2026-109618
- https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w
- https://github.com/9bie/php2shell-bypass-aslr-exp
- https://github.com/xuehuolll/php2shell-CVE-2026-109618-109619/tree/63618bd7629dbfc2d5b505e9dd74e321d8345351
- https://php2shell.ru/
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://github.com/NeoArtemis37/PHP2shell
- https://wiki.astralinux.ru/x/mI0tI
- https://wiki.astralinux.ru/x/k40tI
- https://wiki.astralinux.ru/x/lo0tI
- https://wiki.astralinux.ru/x/no0tI
- https://wiki.astralinux.ru/x/3YwtI
- https://wiki.astralinux.ru/x/jo0tI
- https://wiki.astralinux.ru/x/So8tI
- https://wiki.astralinux.ru/x/d44tI
- https://wiki.astralinux.ru/astra-linux-se18-bulletin-2026-1102SE18HF
- https://wiki.astralinux.ru/astra-linux-se17-bulletin-2026-1109SE17HF
- https://bdu.fstec.ru/vul/2026-17191

Краткое описание: Выполнение произвольного кода в Gitlab

Идентификатор уязвимости: CVE-2026-110264
BDU:2026-17391

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

Уязвимый продукт: Gitlab: от 19.5.0 до 19.5.1

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.

3

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-23 / 2026-10-23

Ссылки на источник:

- https://docs.gitlab.com/releases/patches/patch-release-gitlab-19-5-1-released/
- https://techora.ru/news/gitlab-ispravila-kriticheskuyu-uyazvimost-s-vypolneniem-2026-10-22
- https://hackerone.com/reports/4093475
- https://gitlab.com/gitlab-org/gitlab/-/work_items/633633
- https://github.com/xaviware/go-gitlab-cve-2026-110264-scanner
- https://github.com/TahuCryptsi/poc-gitlab-onigmo-cve-2026-110264
- https://bdu.fstec.ru/vul/2026-17391

4

Краткое описание: Межсайтовый скриптинг в phpMyFAQ

Идентификатор уязвимости: CVE-2026-56736
BDU:2026-15741

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

Уязвимый продукт: phpMyFAQ: до 4.2.0-alpha

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Межсайтовый скриптинг

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-pgwp-vc7q-cvj3
- https://bdu.fstec.ru/vul/2026-15741

Краткое описание: Получение конфиденциальной информации в phpMyFAQ

Идентификатор уязвимости: CVE-2026-56737
BDU:2026-15740

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: phpMyFAQ: от 3.2.0 до 4.1.6

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Получение конфиденциальной информации

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

5

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://github.com/advisories/GHSA-8gpw-xvpf-hvx5
- https://github.com/thorsten/phpMyFAQ/security/advisories/GHSA-8gpw-xvpf-hvx5
- https://github.com/thorsten/phpMyFAQ/commit/410208b90f1d01534812ac5203d3e8d9c7bd591f
- https://github.com/thorsten/phpMyFAQ/commit/5097dff341fb01e93e8561e7261b3ae657df715a
- https://github.com/thorsten/phpMyFAQ/commit/6a69f6e2142fde722165c65b7e0a49f3176e87be
- https://bdu.fstec.ru/vul/2026-15740

6

Краткое описание: Отказ в обслуживании в Wazuh

Идентификатор уязвимости: CVE-2026-71540
BDU:2026-15739

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

Уязвимый продукт: Wazuh: от 3.9.0 до 4.14.7

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: 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://github.com/wazuh/wazuh/commit/9a996bc23d28725f6c1f8f7808355d90e20d3382
- https://github.com/wazuh/wazuh/pull/37280
- https://github.com/wazuh/wazuh/releases/tag/v4.14.7
- https://github.com/wazuh/wazuh/security/advisories/GHSA-78wx-4r6w-w73f
- https://bdu.fstec.ru/vul/2026-15739

Краткое описание: Выполнение произвольного кода в vm2

Идентификатор уязвимости: CVE-2026-100721
BDU:2026-15732

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: vm2: до 3.12.2

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

7

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

Ссылки на источник:

- https://github.com/patriksimek/vm2/security/advisories/GHSA-5h3f-q97h-ccvc
- https://github.com/patriksimek/vm2/commit/6ac3916da84e060c403e407b6b6318fcc66b0e72
- https://github.com/patriksimek/vm2/commit/91034466bfb7f56b95fd48083ec6ca36d058f164
- https://github.com/patriksimek/vm2/commit/ab4ee7d803e8c80155e9eb3672226bddbca4aa9c
- https://github.com/patriksimek/vm2/security/advisories/GHSA-5h3f-q97h-ccvc
- https://bdu.fstec.ru/vul/2026-15732

8

Краткое описание: Отказ в обслуживании в axios

Идентификатор уязвимости: CVE-2026-101903
BDU:2026-15729

Идентификатор программной ошибки: CWE-1018 Управление сессиями пользователей

Уязвимый продукт: axios: от 1.16.1 до 1.20.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://github.com/axios/axios/commit/d19040bda7a8be2f82c3c6e1a5bc03917daee39a
- https://github.com/axios/axios/security/advisories/GHSA-c29m-xwm3-cm6r
- https://bdu.fstec.ru/vul/2026-15729

9

Краткое описание: Получение конфиденциальной информации в axios

Идентификатор уязвимости: CVE-2026-101905
BDU:2026-15727

Идентификатор программной ошибки: CWE-1008 Архитектурные принципы

Уязвимый продукт: axios: от 1.15.2 до 1.20.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://github.com/axios/axios/security/advisories/GHSA-m8m8-qj5v-23w3
- https://github.com/axios/axios/commit/d19040bda7a8be2f82c3c6e1a5bc03917daee39a
- http://github.com/axios/axios/pull/11141
- https://github.com/axios/axios/releases/tag/v1.20.0
- https://bdu.fstec.ru/vul/2026-15727

10

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64508
BDU:2026-15725

Идентификатор программной ошибки: CWE-440 Отклонения от ожидаемого поведения

Уязвимый продукт: Linux: до 7.2-rc2
Red Hat Enterprise Linux: 10
Ubuntu: 26.04 LTS
Debian GNU/Linux: 13
Amazon Linux: 2023

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

Способ эксплуатации: Вероятностные методы.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://access.redhat.com/security/cve/cve-2026-64508
- https://security-tracker.debian.org/tracker/CVE-2026-64508
- https://ubuntu.com/security/CVE-2026-64508
- https://explore.alas.aws.amazon.com/CVE-2026-64508.html
- https://lore.kernel.org/linux-cve-announce/?q=CVE-20
- https://lore.kernel.org/linux-cve-announce/2026072554-CVE-2026-64508-fe26@gregkh/26-64508
- https://git.kernel.org/stable/c/6e52c240c43a601b681e3a4e58fc5685114d4726

- https://git.kernel.org/stable/c/eed774da601268dae674e14d54a15e3624691f52
- https://git.kernel.org/stable/c/8ff183ee4d8c452960df58175a094828c0513b2e
- https://git.kernel.org/stable/c/7a6c171c6a1ac6d1509752dac131d941a3de0b37
- https://git.kernel.org/stable/c/96cce16e26dd02a8678f1e87f88a4b5cdb63b995
- https://www.vusec.net/projects/btr/
- https://bdu.fstec.ru/vul/2026-15725

11

Краткое описание: Обход безопасности в axios

Идентификатор уязвимости: CVE-2026-101898
BDU:2026-15724

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

Уязвимый продукт: axios: от 1.13.0 до 1.20.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 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: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://github.com/axios/axios/security/advisories/GHSA-3pq3-5fj3-cg6v
- https://github.com/axios/axios/commit/d19040bda7a8be2f82c3c6e1a5bc03917daee39a
- https://github.com/axios/axios/pull/11141
- https://github.com/axios/axios/releases/tag/v1.20.0
- https://bdu.fstec.ru/vul/2026-15724

12

Краткое описание: Отказ в обслуживании в axios

Идентификатор уязвимости: CVE-2026-101901
BDU:2026-15723

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

Уязвимый продукт: axios: от 1.13.0 до 1.20.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://github.com/axios/axios/security/advisories/GHSA-542g-h47m-68v8
- https://github.com/axios/axios/commit/d19040bda7a8be2f82c3c6e1a5bc03917daee39a
- https://github.com/axios/axios/pull/11141
- https://github.com/axios/axios/releases/tag/v1.20.0
- https://bdu.fstec.ru/vul/2026-15723

13

Краткое описание: Обход безопасности в axios

Идентификатор уязвимости: CVE-2026-101904
BDU:2026-15722

Идентификатор программной ошибки: CWE-1008 Архитектурные принципы

Уязвимый продукт: axios: от 1.0.0 до 1.20.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://github.com/axios/axios/security/advisories/GHSA-j8rh-479h-cp32
- https://bdu.fstec.ru/vul/2026-15722

14

Краткое описание: Обход безопасности в Catalyst SD-WAN Manager

Идентификатор уязвимости: CVE-2026-76504
BDU:2026-15713

Идентификатор программной ошибки: CWE-177 Некорректная обработка URL-кодировки (шестнадцатеричная кодировка)

Уязвимый продукт: Catalyst SD-WAN Manager: 26.1.2.1_LI_Images

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Обход безопасности

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

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: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-webauth-xr8beuuU
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-76504
- https://www.rapid7.com/blog/post/etr-critical-cisco-catalyst-sd-wan-manager-api-authentication-bypass-exploited-in-the-wild-cve-2026-76504/
- https://bdu.fstec.ru/vul/2026-15713

15

Краткое описание: Выполнение произвольного кода в Wireshark

Идентификатор уязвимости: CVE-2026-95387
BDU:2026-15712

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

Уязвимый продукт: Wireshark: от 4.4.0 до 4.4.18 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://gitlab.com/wireshark/wireshark/-/work_items/21487
- https://www.wireshark.org/security/wnpa-sec-2026-97.html
- https://bdu.fstec.ru/vul/2026-15712

16

Краткое описание: Выполнение произвольного кода в Wireshark

Идентификатор уязвимости: CVE-2026-95389
BDU:2026-15711

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

Уязвимый продукт: Wireshark: от 4.4.0 до 4.4.18 включительно

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://gitlab.com/wireshark/wireshark/-/work_items/21481
- https://www.wireshark.org/security/wnpa-sec-2026-93.html
- https://bdu.fstec.ru/vul/2026-15711

17

Краткое описание: Отказ в обслуживании в axios

Идентификатор уязвимости: CVE-2026-101906
BDU:2026-15726

Идентификатор программной ошибки: CWE-1018 Управление сессиями пользователей

Уязвимый продукт: axios: от 1.15.0 до 1.20.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://github.com/axios/axios/security/advisories/GHSA-mghh-pgcx-3jjj
- https://github.com/axios/axios/commit/d19040bda7a8be2f82c3c6e1a5bc03917daee39a
- http://github.com/axios/axios/pull/11141
- https://github.com/axios/axios/releases/tag/v1.20.0
- https://bdu.fstec.ru/vul/2026-15726

18

Краткое описание: Обход безопасности в PyJWT

Идентификатор уязвимости: CVE-2026-102268
BDU:2026-15800

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: PyJWT: до 2.14.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://github.com/jpadilla/pyjwt/commit/8b4e233a22206b34ec1186e912e75c0b2396ac07
- https://github.com/jpadilla/pyjwt/releases/tag/2.14.0
- https://github.com/jpadilla/pyjwt/security/advisories/GHSA-ffc3-869f-jxw9
- https://github.com/covepseng/cve-2026-102268-poc
- https://bdu.fstec.ru/vul/2026-15800

19

Краткое описание: Внедрение кода в Gitea

Идентификатор уязвимости: CVE-2026-55987
BDU:2026-15831

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: РЕД ОС: 8.0
Gitea: до 1.27.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-02 / 2026-10-02

Ссылки на источник:

- https://github.com/go-gitea/gitea
- https://github.com/go-gitea/gitea/releases/tag/v1.27.0
- https://github.com/go-gitea/gitea/security/advisories/GHSA-vrhc-jjfc-m3m3
- http://repo.red-soft.ru/redos/7.3c/x86_64/updates/
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-15831

20

Краткое описание: Выполнение произвольного кода в Gitea

Идентификатор уязвимости: CVE-2026-54481
BDU:2026-15830

Идентификатор программной ошибки: CWE-295 Некорректная проверка сертификатов

Уязвимый продукт: РЕД ОС: 8.0
Gitea: до 1.27.0
OpenShift Pipelines: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-02 / 2026-10-02

Ссылки на источник:

- https://github.com/go-gitea/gitea
- https://github.com/go-gitea/gitea/releases/tag/v1.27.0
- https://github.com/go-gitea/gitea/security/advisories/GHSA-94v3-77j7-vm48
- https://access.redhat.com/security/cve/CVE-2026-54481
- http://repo.red-soft.ru/redos/7.3c/x86_64/updates/
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-15830

21

Краткое описание: Перезапись произвольных файлов в Gitea

Идентификатор уязвимости: CVE-2026-56443
BDU:2026-15832

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: РЕД ОС: 8.0
Gitea: до 1.27.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Перезапись произвольных файлов

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

Оценка CVSSv3: 9.6 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: 2026-10-02 / 2026-10-02

Ссылки на источник:

- https://github.com/go-gitea/gitea
- https://github.com/go-gitea/gitea/releases/tag/v1.27.0
- https://github.com/go-gitea/gitea/security/advisories/GHSA-7p4h-3gxq-x3h3
- http://repo.red-soft.ru/redos/7.3c/x86_64/updates/
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-15832

22

Краткое описание: Получение конфиденциальной информации в Gitea

Идентификатор уязвимости: CVE-2026-58314
BDU:2026-15833

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

Уязвимый продукт: РЕД ОС: 8.0
Gitea: до 1.27.0
OpenShift Pipelines: -

Категория уязвимого продукта: Прикладное программное обеспечение

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: 7.7 AV:N/AC:L/PR:L/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: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://github.com/go-gitea/gitea
- https://github.com/go-gitea/gitea/releases/tag/v1.27.0
- https://github.com/go-gitea/gitea/security/advisories/GHSA-2fcr-jfvc-vgg2
- https://access.redhat.com/security/cve/CVE-2026-58314
- http://repo.red-soft.ru/redos/7.3c/x86_64/updates/
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-15833

Краткое описание: Получение конфиденциальной информации в Gitea

Идентификатор уязвимости: CVE-2026-58417
BDU:2026-15834

Идентификатор программной ошибки: CWE-706 Некорректное разрешение имени или ссылки

Уязвимый продукт: РЕД ОС: 8.0
Gitea: до 1.27.0
OpenShift Pipelines: -

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

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.

23

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: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://github.com/go-gitea/gitea
- https://github.com/go-gitea/gitea/commit/685b62c60fc595e3612a85f0895471876db56292
- https://github.com/go-gitea/gitea/pull/38145
- https://github.com/go-gitea/gitea/releases/tag/v1.27.0
- https://github.com/go-gitea/gitea/security/advisories/GHSA-jr5x-6h83-wrxf
- https://access.redhat.com/security/cve/CVE-2026-58417
- http://repo.red-soft.ru/redos/7.3c/x86_64/updates/
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-15834

24

Краткое описание: Выполнение произвольного кода в ColdFusion

Идентификатор уязвимости: CVE-2026-48273
BDU:2026-15827

Идентификатор программной ошибки: CWE-95 Некорректная нейтрализация директив в динамически вычисляемом коде (внедрение eval)

Уязвимый продукт: ColdFusion: до 2023.0.23 включительно

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.9 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: 2026-10-02 / 2026-10-02

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb26-119.html
- https://bdu.fstec.ru/vul/2026-15827

25

Краткое описание: Отказ в обслуживании в basic-ftp

Идентификатор уязвимости: CVE-2026-102990
BDU:2026-15797

Идентификатор программной ошибки: CWE-1018 Управление сессиями пользователей

Уязвимый продукт: basic-ftp: до 6.2.0 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-02 / 2026-10-02

Ссылки на источник:

- https://github.com/patrickjuchli/basic-ftp/releases/tag/v6.2.1
- https://github.com/patrickjuchli/basic-ftp/commit/d0d9e07c56e519587bb50532ac6eadbb0cb0cfe9
- https://github.com/patrickjuchli/basic-ftp/security/advisories/GHSA-c475-qrg2-pj4r
- https://bdu.fstec.ru/vul/2026-15797

26

Краткое описание: Перезапись произвольных файлов в PCRE2

Идентификатор уязвимости: CVE-2026-103111
BDU:2026-15794

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: PCRE2: до 10.48 включительно

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Перезапись произвольных файлов

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

Оценка CVSSv3: 7.6 AV:N/AC:L/PR:L/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: 2026-10-02 / 2026-10-02

Ссылки на источник:

- https://github.com/PCRE2Project/pcre2/security/advisories/GHSA-r9hj-j2rw-4q3m
- https://bdu.fstec.ru/vul/2026-15794

27

Краткое описание: Выполнение произвольного кода в Piscina

Идентификатор уязвимости: CVE-2026-102992
BDU:2026-15796

Идентификатор программной ошибки: CWE-1008 Архитектурные принципы

Уязвимый продукт: Piscina: до 6.0.0 rc5

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: 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: 2026-10-02 / 2026-10-02

Ссылки на источник:

- https://github.com/piscinajs/piscina/releases/tag/v4.9.4
- https://github.com/piscinajs/piscina/releases/tag/v5.3.2
- https://github.com/piscinajs/piscina/releases/tag/v6.0.0-rc.5
- https://github.com/piscinajs/piscina/commit/0cb12fca37f526065b072592afe954574dcc656f
- https://github.com/piscinajs/piscina/commit/2f69f67159a0e48b38fd61fa4a91c2fdc19fff72
- https://github.com/piscinajs/piscina/commit/5be7bbb19e3787bb698862cd516121a578d690f7
- https://github.com/piscinajs/piscina/commit/bebbda255c2981cecddd36b171b94be2fd41c9a6
- https://github.com/piscinajs/piscina/security/advisories/GHSA-67c8-pqhq-4rmx
- https://bdu.fstec.ru/vul/2026-15796

28

Краткое описание: Выполнение произвольного кода в FortiMail

Идентификатор уязвимости: CVE-2026-104286
BDU:2026-15790

Идентификатор программной ошибки: CWE-158 Некорректная нейтрализация нулевых байтов или символов NUL

Уязвимый продукт: FortiMail: от 7.2.0 до 7.2.9 включительно

Категория уязвимого продукта: Программно-аппаратное решение

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:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-02 / 2026-10-02

Ссылки на источник:

- https://fortiguard.fortinet.com/psirt/FG-IR-26-175
- https://www.cisa.gov/news-events/alerts/2026/10/01/cisa-adds-one-known-exploited-vulnerability-catalog
- https://www.bleepingcomputer.com/news/security/fortinet-warns-of-critical-fortimail-flaw-exploited-in-zero-day-attacks/
- https://watchtowr.com/intelligence/fortinet-fortimail-cve-2026-104286-faq/
- https://github.com/ShadowForge-Cyber/CVE-2026-104286-POC
- https://bdu.fstec.ru/vul/2026-15790

29

Краткое описание: Получение конфиденциальной информации в РЕД ОС

Идентификатор уязвимости: CVE-2026-58427
BDU:2026-15777

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: РЕД ОС: 8.0
Gitea: до 1.27.0
OpenShift Pipelines: -

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-01 / 2026-10-01

Ссылки на источник:

- https://github.com/go-gitea/gitea
- https://github.com/go-gitea/gitea/releases/tag/v1.27.0
- https://github.com/go-gitea/gitea/security/advisories/GHSA-prr9-9mp4-5gp2
- https://access.redhat.com/security/cve/CVE-2026-58427
- http://repo.red-soft.ru/redos/7.3c/x86_64/updates/
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-15777

30

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83970
BDU:2026-15897

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83970
- https://bdu.fstec.ru/vul/2026-15897

31

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83969
BDU:2026-15896

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83969
- https://bdu.fstec.ru/vul/2026-15896

32

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83967
BDU:2026-15895

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83967
- https://bdu.fstec.ru/vul/2026-15895

33

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83955
BDU:2026-15894

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83955
- https://bdu.fstec.ru/vul/2026-15894

34

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83971
BDU:2026-15898

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83971
- https://bdu.fstec.ru/vul/2026-15898

35

Краткое описание: Выполнение произвольного кода в xrdp

Идентификатор уязвимости: CVE-2026-41252
BDU:2026-15908

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

Уязвимый продукт: Debian GNU/Linux: 13
РЕД ОС: 8.0
xrdp: до 0.10.6.1

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: 9.8 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: 2026-10-02 / 2026-10-02

Ссылки на источник:

- https://github.com/neutrinolabs/XRDP/releases/tag/v0.10.6.1
- https://github.com/neutrinolabs/XRDP/security/advisories/GHSA-w5vg-6qmv-j63j
- https://security-tracker.debian.org/tracker/CVE-2026-41252
- https://deb.freexian.com/extended-lts/tracker/CVE-2026-41252
- http://repo.red-soft.ru/redos/7.3c/x86_64/updates/
- http://repo.red-soft.ru/redos/8.0/x86_64/updates/
- https://bdu.fstec.ru/vul/2026-15908

36

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83974
BDU:2026-15914

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83974
- https://bdu.fstec.ru/vul/2026-15914

37

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83976
BDU:2026-15923

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83976
- https://bdu.fstec.ru/vul/2026-15923

38

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83977
BDU:2026-15926

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83977
- https://bdu.fstec.ru/vul/2026-15926

39

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83978
BDU:2026-15931

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83978
- https://bdu.fstec.ru/vul/2026-15931

40

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83972
BDU:2026-15899

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83972
- https://bdu.fstec.ru/vul/2026-15899

41

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83980
BDU:2026-15934

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83980
- https://bdu.fstec.ru/vul/2026-15934

42

Краткое описание: Отказ в обслуживании в NetScaler Gateway

Идентификатор уязвимости: CVE-2026-88779
BDU:2026-15858

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

Уязвимый продукт: NetScaler Gateway: от 13.1 до 13.1-64.28
NetScaler ADC FIPS: до 13.1-37.282
NetScaler ADC NDcPP: до 13.1-37.282
NetScaler ADC: от 13.1 до 13.1-64.28

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX697174
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-88779
- https://community.citrix.com/techzone-blogs/110_security-updates/understanding-and-addressing-cve-2026-88779-in-citrix-netscaler-adc-and-citrix-netscaler-gateway/
- https://www.cisa.gov/sites/default/files/csv/known_exploited_vulnerabilities.csv
- https://bdu.fstec.ru/vul/2026-15858

43

Краткое описание: Обход безопасности в simple-git

Идентификатор уязвимости: CVE-2026-102829
BDU:2026-15880

Идентификатор программной ошибки: CWE-184 Неполный черный список

Уязвимый продукт: simple-git: до 2.0.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 9.8 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: 2026-10-02 / 2026-10-02

Ссылки на источник:

- https://github.com/steveukx/git-js/security/advisories/GHSA-v5rq-49vh-5v5c
- https://github.com/steveukx/git-js/commit/68874c239f0c7a87f4a68c3d2c4a0d7c75bb27f4
- https://github.com/steveukx/git-js/pull/1201
- http://github.com/steveukx/git-js/releases/tag/@simple-git/argv-parser@2.0.1
- https://bdu.fstec.ru/vul/2026-15880

44

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83981
BDU:2026-15935

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83981
- https://bdu.fstec.ru/vul/2026-15935

45

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83983
BDU:2026-15937

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83983
- https://bdu.fstec.ru/vul/2026-15937

46

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83982
BDU:2026-15936

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83982
- https://bdu.fstec.ru/vul/2026-15936

47

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83975
BDU:2026-15965

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83975
- https://bdu.fstec.ru/vul/2026-15965

48

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83973
BDU:2026-15964

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83973
- https://bdu.fstec.ru/vul/2026-15964

Краткое описание: Чтение локальных файлов в Tornado

Идентификатор уязвимости: CVE-2026-103263
BDU:2026-15963

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

Уязвимый продукт: Tornado: до 6.5.9

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Манипулирование ресурсами.

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.

49

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://github.com/tornadoweb/tornado/commit/437ab5f76565403b3403438d2e555d11f8128d32
- https://github.com/tornadoweb/tornado/security/advisories/GHSA-c2m8-h5v5-343r
- https://www.vulncheck.com/advisories/tornado-before-6.5.9-staticfilehandler-path-traversal-via-symlink
- https://bdu.fstec.ru/vul/2026-15963

50

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83968
BDU:2026-15940

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 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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83968
- https://bdu.fstec.ru/vul/2026-15940

51

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83979
BDU:2026-15939

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 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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83979
- https://bdu.fstec.ru/vul/2026-15939

52

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83985
BDU:2026-15938

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: 2026-10-05 / 2026-10-05

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83985
- https://bdu.fstec.ru/vul/2026-15938

53

Краткое описание: Обход безопасности в Visual Studio Code

Идентификатор уязвимости: CVE-2026-81379
BDU:2026-15988

Идентификатор программной ошибки: CWE-636 Небезопасное восстановление после сбоя (сбой с открытием доступа)

Уязвимый продукт: Visual Studio Code: до 1.136.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование сроками и состоянием.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81379
- https://bdu.fstec.ru/vul/2026-15988

Краткое описание: Повышение привилегий в Windows Virtualization-Based Security Enclave

Идентификатор уязвимости: CVE-2026-83498
BDU:2026-15990

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Windows 11 23H2: до 10.0.22631.7582
Windows 11 24H2: до 10.0.26100.9445
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.

54

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83498
- https://bdu.fstec.ru/vul/2026-15990

55

Краткое описание: Повышение привилегий в Windows Secure Kernel Mode

Идентификатор уязвимости: CVE-2026-83939
BDU:2026-15991

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: 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: 8.2 AV:L/AC:L/PR:H/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: 2026-10-06 / 2026-10-06

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83939
- https://bdu.fstec.ru/vul/2026-15991

56

Краткое описание: Повышение привилегий в Windows Kernel

Идентификатор уязвимости: CVE-2026-83942
BDU:2026-15993

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: 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 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: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83942
- https://bdu.fstec.ru/vul/2026-15993

57

Краткое описание: Повышение привилегий в Windows Hello

Идентификатор уязвимости: CVE-2026-81354
BDU:2026-15998

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

Уязвимый продукт: 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 2019: до 10.0.17763.9245
Windows Server 2019 (Server Core installation): до 10.0.17763.9245
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: 8.2 AV:L/AC:L/PR:H/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: 2026-10-06 / 2026-10-06

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81354
- https://bdu.fstec.ru/vul/2026-15998

58

Краткое описание: Повышение привилегий в Windows Remote Desktop Services

Идентификатор уязвимости: CVE-2026-80096
BDU:2026-15996

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: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80096
- https://bdu.fstec.ru/vul/2026-15996

59

Краткое описание: Выполнение произвольного кода в Virtual Hard Disk Miniport Driver

Идентификатор уязвимости: CVE-2026-81355
BDU:2026-15997

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: 7.5 AV:L/AC:H/PR:H/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: 2026-10-06 / 2026-10-06

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81355
- https://bdu.fstec.ru/vul/2026-15997

60

Краткое описание: Выполнение произвольного кода в Windows Hyper-V

Идентификатор уязвимости: CVE-2026-80083
BDU:2026-16000

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

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: Выполнение произвольного кода

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80083
- https://bdu.fstec.ru/vul/2026-16000

61

Краткое описание: Обход безопасности в Visual Studio Code

Идентификатор уязвимости: CVE-2026-81378
BDU:2026-15987

Идентификатор программной ошибки: CWE-436 Конфликт интерпретации

Уязвимый продукт: Visual Studio Code: до 1.136.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Анализ целевого объекта

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81378
- https://bdu.fstec.ru/vul/2026-15987

62

Краткое описание: Повышение привилегий в Windows Resilient File System

Идентификатор уязвимости: CVE-2026-83952
BDU:2026-15994

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

Уязвимый продукт: Windows 11 24H2: до 10.0.26100.9445
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: 2026-10-06 / 2026-10-06

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83952
- https://bdu.fstec.ru/vul/2026-15994

63

Краткое описание: Обход безопасности в Visual Studio Code

Идентификатор уязвимости: CVE-2026-81357
BDU:2026-15986

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

Уязвимый продукт: Visual Studio Code: до 1.136.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81357
- https://bdu.fstec.ru/vul/2026-15986

64

Краткое описание: Повышение привилегий в PowerLogic T300

Идентификатор уязвимости: CVE-2026-77120
BDU:2026-15982

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

Уязвимый продукт: PowerLogic T300: до 2.9.8-5621

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Инъекция.

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: 8.2 AV:L/AC:L/PR:H/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: 2026-09-17 / 2026-09-17

Ссылки на источник:

- https://download.se.com/files?p_Doc_Ref=SEVD-2026-251-02&p_enDocType=Security+and+Safety+Notice&p_File_Name=SEVD-2026-251-02.pdf
- https://bdu.fstec.ru/vul/2026-15982

65

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-83954
BDU:2026-15984

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-83954
- https://bdu.fstec.ru/vul/2026-15984

66

Краткое описание: Обход безопасности в Visual Studio Code

Идентификатор уязвимости: CVE-2026-81356
BDU:2026-15985

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

Уязвимый продукт: Visual Studio Code: до 1.136.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-81356
- https://bdu.fstec.ru/vul/2026-15985

67

Краткое описание: Выполнение произвольного кода в Libheif

Идентификатор уязвимости: BDU:2026-15971

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: WordPress: 7.1.0
Libheif: от 1.18.0 до 1.23.2 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: 2026-10-06 / 2026-10-06

Ссылки на источник:

- https://github.com/strukturag/libheif/security/advisories/GHSA-x8r2-mggj-j6wr
- https://fortbridge.co.uk/research/wordpress-libheif-rce/
- https://bdu.fstec.ru/vul/2026-15971

68

Краткое описание: Выполнение произвольного кода в Windows Routing and Remote Access Service

Идентификатор уязвимости: CVE-2026-72959
BDU:2026-15974

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72959
- https://bdu.fstec.ru/vul/2026-15974

69

Краткое описание: Выполнение произвольного кода в Windows Media Player

Идентификатор уязвимости: CVE-2026-72960
BDU:2026-15975

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72960
- https://bdu.fstec.ru/vul/2026-15975

70

Краткое описание: Повышение привилегий в Windows Hyper-V

Идентификатор уязвимости: CVE-2026-72961
BDU:2026-15976

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: 8.2 AV:L/AC:L/PR:H/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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72961
- https://bdu.fstec.ru/vul/2026-15976

71

Краткое описание: Выполнение произвольного кода в piwigo

Идентификатор уязвимости: CVE-2026-42322
BDU:2026-15970

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

Уязвимый продукт: piwigo: до 16.4.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Злоупотребление функционалом.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.1 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: 2026-10-06 / 2026-10-06

Ссылки на источник:

- https://github.com/Piwigo/Piwigo/commit/1e7f7262cb30e6916779f93e66d5d6579ec75a11
- https://github.com/Piwigo/Piwigo/commit/4a13ec9a8f4881ae1f23bdfd24d7b90cd0802cdc
- https://github.com/Piwigo/Piwigo/releases/tag/16.4.0
- https://github.com/Piwigo/Piwigo/security/advisories/GHSA-7w97-5g4p-xqvv
- https://github.com/LipeOzyy/CVE-2026-42322
- https://bdu.fstec.ru/vul/2026-15970

72

Краткое описание: Выполнение произвольного кода в Linux

Идентификатор уязвимости: CVE-2026-64074
BDU:2026-15980

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Linux: 7.1 rc4
Ubuntu: 26.04 LTS
ПК «Горизонт-ВС»: 40-17-37-17

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

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://dbugs.ptsecurity.com/pt/vulnerability/PT-2026-61391
- https://ubuntu.com/security/CVE-2026-64074
- https://git.kernel.org/stable/c/e37ea2c6f17f273813ea4e8e94c102591d598ce1
- https://git.kernel.org/stable/c/a3bf0f28d4ba16e1f35f8c983bb04426b87e2a78
- https://git.kernel.org/stable/c/93614949dc86f068e3c32c32cf1ee2a2323177a7
- https://wiki.pangeo-gorizont.ru/docs/byulleteni-bezopasnosti
- https://bdu.fstec.ru/vul/2026-15980

73

Краткое описание: Выполнение произвольного кода в PTC Windchill PDMLink и PTC FlexPLM

Идентификатор уязвимости: CVE-2026-12569
BDU:2026-15983

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: PTC Windchill PDMlink: до 11.0 M030
PTC FlexPLM: до 11.0 M030

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-10-06 / 2026-10-06

Ссылки на источник:

- https://www.ptc.com/en/support/article/CS473270
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2026-12569
- https://bdu.fstec.ru/vul/2026-15983

74

Краткое описание: Повышение привилегий в Windows USB Video Driver

Идентификатор уязвимости: CVE-2026-72962
BDU:2026-15977

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

Уязвимый продукт: 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 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: 8.2 AV:L/AC:L/PR:H/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://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-72962
- https://bdu.fstec.ru/vul/2026-15977

75

Краткое описание: Повышение привилегий в Windows Work Folders

Идентификатор уязвимости: CVE-2026-80075
BDU:2026-16017

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 R2: до 6.3.9600.23398
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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80075
- https://bdu.fstec.ru/vul/2026-16017

76

Краткое описание: Выполнение произвольного кода в Microsoft Failover Cluster

Идентификатор уязвимости: CVE-2026-78444
BDU:2026-16033

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

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 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78444
- https://bdu.fstec.ru/vul/2026-16033

77

Краткое описание: Выполнение произвольного кода в Windows OLE DB

Идентификатор уязвимости: CVE-2026-78442
BDU:2026-16032

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

Уязвимый продукт: Microsoft SQL Server 2019 (CU 32): до 15.0.4490.9
Microsoft SQL Server 2017 (CU 31): до 14.0.3550.4
Microsoft SQL Server 2019 (GDR): до 15.0.2190.7
Microsoft SQL Server 2017 (GDR): до 14.0.2130.4

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: 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78442
- https://bdu.fstec.ru/vul/2026-16032

78

Краткое описание: Выполнение произвольного кода в Microsoft Office Graphics Component

Идентификатор уязвимости: CVE-2026-78439
BDU:2026-16031

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Microsoft Office: до 16.0.20430.20000
Microsoft Office LTSC 2021: до 16.113.26091433
Microsoft Office LTSC 2024: до 16.113.26091433
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:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78439
- https://bdu.fstec.ru/vul/2026-16031

79

Краткое описание: Получение конфиденциальной информации в Azure CycleCloud

Идентификатор уязвимости: CVE-2026-77909
BDU:2026-16030

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

Уязвимый продукт: Azure CycleCloud: до 8.9.2

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 7.7 AV:N/AC:L/PR:L/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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77909
- https://bdu.fstec.ru/vul/2026-16030

80

Краткое описание: Выполнение произвольного кода в Microsoft Dynamics 365 On-Premises

Идентификатор уязвимости: CVE-2026-77908
BDU:2026-16029

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

Уязвимый продукт: Microsoft Dynamics 365 Customer Engagement: до 9.1.0048.0004

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77908
- https://bdu.fstec.ru/vul/2026-16029

81

Краткое описание: Выполнение произвольного кода в Visual Studio

Идентификатор уязвимости: CVE-2026-77907
BDU:2026-16028

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

Уязвимый продукт: Microsoft Visual Studio 2026: от 18.9 до 18.9.3

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77907
- https://bdu.fstec.ru/vul/2026-16028

82

Краткое описание: Выполнение произвольного кода в Visual Studio

Идентификатор уязвимости: CVE-2026-77906
BDU:2026-16027

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

Уязвимый продукт: Microsoft Visual Studio 2026: от 18.9 до 18.9.3

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77906
- https://bdu.fstec.ru/vul/2026-16027

83

Краткое описание: Выполнение произвольного кода в Windows Remote Desktop Client

Идентификатор уязвимости: CVE-2026-80077
BDU:2026-16019

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

Уязвимый продукт: Microsoft Remote Desktop Client for Windows: до 1.2.7279.0

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80077
- https://bdu.fstec.ru/vul/2026-16019

84

Краткое описание: Выполнение произвольного кода в Windows Remote Desktop Client

Идентификатор уязвимости: CVE-2026-80074
BDU:2026-16018

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

Уязвимый продукт: Microsoft Remote Desktop Client for Windows: до 1.2.7279.0

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-80074
- https://bdu.fstec.ru/vul/2026-16018

85

Краткое описание: Получение конфиденциальной информации в Atlassian Data Center

Идентификатор уязвимости: CVE-2026-21589
BDU:2026-16016

Идентификатор программной ошибки: CWE-552 Непредусмотренный доступ к файлам или каталогам

Уязвимый продукт: Jira Service Management Data Center: до 5.12.40
Bitbucket Data Center: до 9.4.26
Bamboo Data Center: до 12.1.12
Confluence Data Center: до 9.2.26
Crowd Data Center: до 6.3.7
Crucible Data Center: до 4.9.15
Fisheye Data Center: до 4.9.15
Jira Software Data Center: до 9.12.40

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Несанкционированный сбор информации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://github.com/tc4dy/CVE-2026-21589-PoC-Exploit
- https://jira.atlassian.com/browse/BAM-26567
- https://jira.atlassian.com/browse/BSERV-20604
- https://jira.atlassian.com/browse/CONFSERVER-104488

- https://jira.atlassian.com/browse/CRUC-8741
- https://jira.atlassian.com/browse/CWD-6610
- https://jira.atlassian.com/browse/FE-7583
- https://jira.atlassian.com/browse/JRASERVER-79546
- https://jira.atlassian.com/browse/JSDSERVER-16809
- https://bdu.fstec.ru/vul/2026-16016

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-78505
BDU:2026-16002

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 16.0.5569.1000
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.

86

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78505
- https://bdu.fstec.ru/vul/2026-16002

Краткое описание: Выполнение произвольного кода в TeamViewer

Идентификатор уязвимости: CVE-2026-16444
BDU:2026-16014

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

Уязвимый продукт: TeamViewer Host: до 13.2.153981
TeamViewer Full Client: до 13.2.153981
TeamViewer QuickSupport: до 14.7.48839
TeamViewer Portable: до 15.64.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://www.teamviewer.com/de/resources/trust-center/security-bulletins/tv-2026-1008/
- https://github.com/jamir0quai/CVE-2026-16444
- https://bdu.fstec.ru/vul/2026-16014

88

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-78504
BDU:2026-16001

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 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:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78504
- https://bdu.fstec.ru/vul/2026-16001

89

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-78512
BDU:2026-16004

Идентификатор программной ошибки: CWE-197 Ошибка числовых усечений

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:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78512
- https://bdu.fstec.ru/vul/2026-16004

90

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-78517
BDU:2026-16005

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 16.0.5569.1000
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:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78517
- https://bdu.fstec.ru/vul/2026-16005

91

Краткое описание: Выполнение произвольного кода в Microsoft Office Excel

Идентификатор уязвимости: CVE-2026-78518
BDU:2026-16006

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: 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78518
- https://bdu.fstec.ru/vul/2026-16006

92

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-78511
BDU:2026-16003

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 16.0.5569.1000
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:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78511
- https://bdu.fstec.ru/vul/2026-16003

93

Краткое описание: Выполнение произвольного кода в Microsoft Office Outlook

Идентификатор уязвимости: CVE-2026-78519
BDU:2026-16008

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

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 Outlook 2016: до 16.0.5569.1000

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Манипулирование ресурсами.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78519
- https://bdu.fstec.ru/vul/2026-16008

94

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-78507
BDU:2026-16009

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 Office LTSC 2024: до 16.0.17932.20976
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:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78507
- https://bdu.fstec.ru/vul/2026-16009

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-78514
BDU:2026-16010

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 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.

95

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78514
- https://bdu.fstec.ru/vul/2026-16010

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-78521
BDU:2026-16007

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 16.0.5569.1000
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.

96

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78521
- https://bdu.fstec.ru/vul/2026-16007

97

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-77489
BDU:2026-16072

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77489
- https://bdu.fstec.ru/vul/2026-16072

98

Краткое описание: Отказ в обслуживании в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-77494
BDU:2026-16064

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

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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77494
- https://bdu.fstec.ru/vul/2026-16064

99

Краткое описание: Отказ в обслуживании в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-77498
BDU:2026-16065

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 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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77498
- https://bdu.fstec.ru/vul/2026-16065

100

Краткое описание: Выполнение произвольного кода в Windows Imaging Component

Идентификатор уязвимости: CVE-2026-77495
BDU:2026-16066

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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77495
- https://bdu.fstec.ru/vul/2026-16066

101

Краткое описание: Выполнение произвольного кода в Windows Reliable Multicast Transport Driver

Идентификатор уязвимости: CVE-2026-78450
BDU:2026-16067

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78450
- https://bdu.fstec.ru/vul/2026-16067

102

Краткое описание: Выполнение произвольного кода в Windows Reliable Multicast Transport Driver

Идентификатор уязвимости: CVE-2026-78449
BDU:2026-16068

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78449
- https://bdu.fstec.ru/vul/2026-16068

103

Краткое описание: Отказ в обслуживании в excelize

Идентификатор уязвимости: CVE-2026-107213
BDU:2026-16070

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: excelize: от 2.9.0 до 2.11.0 включительно

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:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://github.com/qax-os/excelize/commit/8ffeb07ec9a350410f6922313f6b7e4f5cc79241
- https://github.com/qax-os/excelize/pull/2434
- https://github.com/qax-os/excelize/security/advisories/GHSA-r7x5-4969-99p7
- https://bdu.fstec.ru/vul/2026-16070

104

Краткое описание: Повышение привилегий в SQL Server

Идентификатор уязвимости: CVE-2026-77487
BDU:2026-16073

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Microsoft SQL Server 2025 (GDR): до 17.0.1135.8
Microsoft SQL Server 2022 (GDR): до 16.0.1200.5
Microsoft SQL Server 2019 (CU 32): до 15.0.4490.9
Microsoft SQL Server 2017 (CU 31): до 14.0.3550.4
Microsoft SQL Server 2019 (GDR): до 15.0.2190.7
Microsoft SQL Server 2017 (GDR): до 14.0.2130.4
Microsoft SQL Server 2022 (CU 26): до 16.0.4275.2
Microsoft SQL Server 2025 (CU8): до 17.0.4085.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77487
- https://bdu.fstec.ru/vul/2026-16073

105

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-73011
BDU:2026-16079

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73011
- https://bdu.fstec.ru/vul/2026-16079

Краткое описание: Повышение привилегий в SQL Server

Идентификатор уязвимости: CVE-2026-77483
BDU:2026-16075

Идентификатор программной ошибки: CWE-1038 Небезопасная автоматическая оптимизация

Уязвимый продукт: Microsoft SQL Server 2025 (GDR): до 17.0.1135.8
Microsoft SQL Server 2022 (GDR): до 16.0.1200.5
Microsoft SQL Server 2019 (CU 32): до 15.0.4490.9
Microsoft SQL Server 2019 (GDR): до 15.0.2190.7
Microsoft SQL Server 2022 (CU 26): до 16.0.4275.2
Microsoft SQL Server 2025 (CU8): до 17.0.4085.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение аутентификации.

106 **Последствия эксплуатации:** Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77483
- https://bdu.fstec.ru/vul/2026-16075

Краткое описание: Повышение привилегий в SQL Server

Идентификатор уязвимости: CVE-2026-77480
BDU:2026-16076

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

Уязвимый продукт: Microsoft SQL Server 2025 (GDR): до 17.0.1135.8
Microsoft SQL Server 2022 (GDR): до 16.0.1200.5
Microsoft SQL Server 2019 (CU 32): до 15.0.4490.9
Microsoft SQL Server 2017 (CU 31): до 14.0.3550.4
Microsoft SQL Server 2019 (GDR): до 15.0.2190.7
Microsoft SQL Server 2017 (GDR): до 14.0.2130.4
Microsoft SQL Server 2022 (CU 26): до 16.0.4275.2
Microsoft SQL Server 2025 (CU8): до 17.0.4085.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

107

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77480
- https://bdu.fstec.ru/vul/2026-16076

108

Краткое описание: Повышение привилегий в SQL Server

Идентификатор уязвимости: CVE-2026-73028
BDU:2026-16077

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Microsoft SQL Server 2025 (GDR): до 17.0.1135.8
Microsoft SQL Server 2022 (GDR): до 16.0.1200.5
Microsoft SQL Server 2019 (CU 32): до 15.0.4490.9
Microsoft SQL Server 2017 (CU 31): до 14.0.3550.4
Microsoft SQL Server 2019 (GDR): до 15.0.2190.7
Microsoft SQL Server 2017 (GDR): до 14.0.2130.4
Microsoft SQL Server 2022 (CU 26): до 16.0.4275.2
Microsoft SQL Server 2025 (CU8): до 17.0.4085.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73028
- https://bdu.fstec.ru/vul/2026-16077

109

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-73007
BDU:2026-16078

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73007
- https://bdu.fstec.ru/vul/2026-16078

110

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-73015
BDU:2026-16080

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73015
- https://bdu.fstec.ru/vul/2026-16080

111

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-73020
BDU:2026-16081

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73020
- https://bdu.fstec.ru/vul/2026-16081

112

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-73021
BDU:2026-16082

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73021
- https://bdu.fstec.ru/vul/2026-16082

113

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-73026
BDU:2026-16083

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73026
- https://bdu.fstec.ru/vul/2026-16083

114

Краткое описание: Выполнение произвольного кода в SQL Server

Идентификатор уязвимости: CVE-2026-78456
BDU:2026-16063

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

Уязвимый продукт: Microsoft SQL Server 2022 (GDR): до 16.0.1200.5
Microsoft SQL Server 2022 (CU 26): до 16.0.4275.2

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: 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78456
- https://bdu.fstec.ru/vul/2026-16063

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server

Идентификатор уязвимости: CVE-2026-77484
BDU:2026-16074

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft SQL Server 2025 (GDR): до 17.0.1135.8
Microsoft SQL Server 2022 (GDR): до 16.0.1200.5
Microsoft SQL Server 2019 (CU 32): до 15.0.4490.9
Microsoft SQL Server 2019 (GDR): до 15.0.2190.7
Microsoft SQL Server 2022 (CU 26): до 16.0.4275.2
Microsoft SQL Server 2025 (CU8): до 17.0.4085.5

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

115 **Последствия эксплуатации:** Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77484
- https://bdu.fstec.ru/vul/2026-16074

116

Краткое описание: Выполнение произвольного кода в Windows Remote Desktop Client

Идентификатор уязвимости: CVE-2026-78463
BDU:2026-16061

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

Уязвимый продукт: Remote Desktop client for Windows Desktop: до 1.2.7279.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 AV:N/AC:L/PR: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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78463
- https://bdu.fstec.ru/vul/2026-16061

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-77901
BDU:2026-16051

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

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:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77901
- https://bdu.fstec.ru/vul/2026-16051

118

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-78447
BDU:2026-16057

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78447
- https://bdu.fstec.ru/vul/2026-16057

119

Краткое описание: Обход безопасности в Visual Studio Code

Идентификатор уязвимости: CVE-2026-78462
BDU:2026-16060

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

Уязвимый продукт: Visual Studio Code: до 1.136.2

Категория уязвимого продукта: Прикладное программное обеспечение

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: 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78462
- https://bdu.fstec.ru/vul/2026-16060

120

Краткое описание: Выполнение произвольного кода в Apache ActiveMQ Artemis и Apache Artemis

Идентификатор уязвимости: CVE-2026-57967
BDU:2026-16034

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

Уязвимый продукт: ActiveMQ Artemis: от 2.50.0 до 2.56.0 включительно
Artemis: от 1.0.0 до 2.44.0 включительно

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://github.com/c0dem4sters/CVE-2026-57967
- https://issues.apache.org/jira/browse/ARTEMIS-6245
- https://github.com/apache/artemis/commit/26ce5813dc9d640b18f18c436801454e0192895c
- https://lists.apache.org/thread/fxfjqrdsnksw5f17zs3yqo864lblgv6y
- https://bdu.fstec.ru/vul/2026-16034

121

Краткое описание: Выполнение произвольного кода в shell-quote

Идентификатор уязвимости: CVE-2026-102422
BDU:2026-16035

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

Уязвимый продукт: shell-quote: от 1.8.4 до 1.11.0

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Инъекция.

Последствия эксплуатации: Выполнение произвольного кода

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

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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://github.com/ljharb/shell-quote/commit/6002b2ed90c6b83095eb272b6b0adaf3a172b0bc
- https://github.com/ljharb/shell-quote/security/advisories/GHSA-pqg4-j6r4-53mv
- https://www.npmjs.com/package/shell-quote
- https://github.com/DevVaibhav07/CVE-2026-102422
- https://bdu.fstec.ru/vul/2026-16035

122

Краткое описание: Повышение привилегий в Windows Device Association Service

Идентификатор уязвимости: CVE-2026-77500
BDU:2026-16037

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

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 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77500
- https://bdu.fstec.ru/vul/2026-16037

123

Краткое описание: Отказ в обслуживании в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-77502
BDU:2026-16039

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 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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77502
- https://bdu.fstec.ru/vul/2026-16039

124

Краткое описание: Отказ в обслуживании в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-77886
BDU:2026-16040

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 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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77886
- https://bdu.fstec.ru/vul/2026-16040

125

Краткое описание: Отказ в обслуживании в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-77893
BDU:2026-16041

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 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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77893
- https://bdu.fstec.ru/vul/2026-16041

126

Краткое описание: Отказ в обслуживании в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-77895
BDU:2026-16042

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 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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77895
- https://bdu.fstec.ru/vul/2026-16042

127

Краткое описание: Отказ в обслуживании в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-77501
BDU:2026-16038

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 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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77501
- https://bdu.fstec.ru/vul/2026-16038

128

Краткое описание: Отказ в обслуживании в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-77889
BDU:2026-16044

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

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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77889
- https://bdu.fstec.ru/vul/2026-16044

129

Краткое описание: Отказ в обслуживании в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-77888
BDU:2026-16045

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

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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77888
- https://bdu.fstec.ru/vul/2026-16045

130

Краткое описание: Выполнение произвольного кода в Windows DNS Server

Идентификатор уязвимости: CVE-2026-77505
BDU:2026-16046

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: 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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77505
- https://bdu.fstec.ru/vul/2026-16046

131

Краткое описание: Повышение привилегий в Windows NTFS

Идентификатор уязвимости: CVE-2026-77503
BDU:2026-16047

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77503
- https://bdu.fstec.ru/vul/2026-16047

132

Краткое описание: Выполнение произвольного кода в Microsoft Office Word

Идентификатор уязвимости: CVE-2026-77504
BDU:2026-16048

Идентификатор программной ошибки: CWE-415 Двойное освобождение

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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77504
- https://bdu.fstec.ru/vul/2026-16048

133

Краткое описание: Повышение привилегий в Windows Volume Manager Extension Driver

Идентификатор уязвимости: CVE-2026-77904
BDU:2026-16050

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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77904
- https://bdu.fstec.ru/vul/2026-16050

134

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2026-77898
BDU:2026-16053

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77898
- https://bdu.fstec.ru/vul/2026-16053

135

Краткое описание: Отказ в обслуживании в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-77499
BDU:2026-16055

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

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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77499
- https://bdu.fstec.ru/vul/2026-16055

136

Краткое описание: Отказ в обслуживании в Windows DHCP Server

Идентификатор уязвимости: CVE-2026-77890
BDU:2026-16043

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

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: 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: 2026-10-08 / 2026-10-08

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77890
- https://bdu.fstec.ru/vul/2026-16043

137

Краткое описание: Повышение привилегий в Windows Biometric Service

Идентификатор уязвимости: CVE-2026-78448
BDU:2026-16056

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-78448
- https://bdu.fstec.ru/vul/2026-16056

138

Краткое описание: Повышение привилегий в Data Sharing Service Client

Идентификатор уязвимости: CVE-2026-73014
BDU:2026-16084

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

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: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73014
- https://bdu.fstec.ru/vul/2026-16084

139

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server

Идентификатор уязвимости: CVE-2026-77486
BDU:2026-16085

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

Уязвимый продукт: Microsoft SQL Server 2019 (CU 32): до 15.0.4490.9
Microsoft SQL Server 2017 (CU 31): до 14.0.3550.4
Microsoft SQL Server 2019 (GDR): до 15.0.2190.7
Microsoft SQL Server 2017 (GDR): до 14.0.2130.4

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: 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77486
- https://bdu.fstec.ru/vul/2026-16085

140

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server

Идентификатор уязвимости: CVE-2026-77482
BDU:2026-16087

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

Уязвимый продукт: Microsoft SQL Server 2019 (CU 32): до 15.0.4490.9
Microsoft SQL Server 2017 (CU 31): до 14.0.3550.4
Microsoft SQL Server 2019 (GDR): до 15.0.2190.7
Microsoft SQL Server 2017 (GDR): до 14.0.2130.4

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: 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77482
- https://bdu.fstec.ru/vul/2026-16087

141

Краткое описание: Выполнение произвольного кода в Microsoft SQL Server

Идентификатор уязвимости: CVE-2026-77481
BDU:2026-16088

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

Уязвимый продукт: Microsoft SQL Server 2025 (GDR): до 17.0.1135.8
Microsoft SQL Server 2022 (GDR): до 16.0.1200.5
Microsoft SQL Server 2019 (CU 32): до 15.0.4490.9
Microsoft SQL Server 2017 (CU 31): до 14.0.3550.4
Microsoft SQL Server 2019 (GDR): до 15.0.2190.7
Microsoft SQL Server 2017 (GDR): до 14.0.2130.4
Microsoft SQL Server 2022 (CU 26): до 16.0.4275.2
Microsoft SQL Server 2025 (CU8): до 17.0.4085.5

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: 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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-77481
- https://bdu.fstec.ru/vul/2026-16088

142

Краткое описание: Выполнение произвольного кода в Windows Imaging Component

Идентификатор уязвимости: CVE-2026-73023
BDU:2026-16089

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73023
- https://bdu.fstec.ru/vul/2026-16089

143

Краткое описание: Выполнение произвольного кода в Windows Imaging Component

Идентификатор уязвимости: CVE-2026-73013
BDU:2026-16090

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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73013
- https://bdu.fstec.ru/vul/2026-16090

144

Краткое описание: Повышение привилегий в Windows Management Services

Идентификатор уязвимости: CVE-2026-73012
BDU:2026-16091

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: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: 2026-10-07 / 2026-10-07

Ссылки на источник:

- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-73012
- https://bdu.fstec.ru/vul/2026-16091

145

Краткое описание: Выполнение произвольного кода в Cisco APIC

Идентификатор уязвимости: CVE-2026-76500
BDU:2026-16093

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

Уязвимый продукт: Cisco APIC: от 6.2 до 6.2(3g)

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2026-10-09 / 2026-10-09

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-apic-UOXWtfh
- https://bdu.fstec.ru/vul/2026-16093

146

Краткое описание: Выполнение произвольного кода в Cisco APIC

Идентификатор уязвимости: CVE-2026-76499
BDU:2026-16094

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

Уязвимый продукт: Cisco APIC: от 6.2 до 6.2(3g)

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Манипулирование структурами данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-09 / 2026-10-09

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-apic-UOXWtfh
- https://bdu.fstec.ru/vul/2026-16094

147

Краткое описание: Выполнение произвольного кода в Cisco APIC

Идентификатор уязвимости: CVE-2026-76498
BDU:2026-16095

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Cisco APIC: от 6.2 до 6.2(3g)

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-09 / 2026-10-09

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-apic-UOXWtfh
- https://bdu.fstec.ru/vul/2026-16095

148

Краткое описание: Выполнение произвольного кода в NX-OS

Идентификатор уязвимости: CVE-2026-76486
BDU:2026-16097

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: NX-OS: 10.6(3s)

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 2026-10-09 / 2026-10-09

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ngoam-rce-LWKQ4BU
- https://bdu.fstec.ru/vul/2026-16097

149

Краткое описание: Выполнение произвольного кода в NX-OS

Идентификатор уязвимости: CVE-2026-76485
BDU:2026-16098

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: NX-OS: 10.6(3s)

Категория уязвимого продукта: Телекоммуникационное оборудование

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: 2026-10-09 / 2026-10-09

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ngoam-rce-LWKQ4BU
- https://bdu.fstec.ru/vul/2026-16098

150

Краткое описание: Выполнение произвольного кода в Cisco Smart Software Manager On-Prem

Идентификатор уязвимости: CVE-2026-76484
BDU:2026-16099

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

Уязвимый продукт: Cisco Smart Software Manager On-Prem: до 10-202609
Cisco License On-Prem: до 10-202609

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: 2026-10-09 / 2026-10-09

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ssm-Ph77wdhf
- https://bdu.fstec.ru/vul/2026-16099

151

Краткое описание: Выполнение произвольного кода в Cisco Smart Software Manager On-Prem

Идентификатор уязвимости: CVE-2026-76480
BDU:2026-16100

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

Уязвимый продукт: Cisco Smart Software Manager On-Prem: до 10-202609
Cisco License On-Prem: до 10-202609

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: 2026-10-09 / 2026-10-09

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ssm-Ph77wdhf
- https://bdu.fstec.ru/vul/2026-16100

152

Краткое описание: Выполнение произвольного кода в Cisco Smart Software Manager On-Prem

Идентификатор уязвимости: CVE-2026-76482
BDU:2026-16101

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: Cisco Smart Software Manager On-Prem: до 10-202609
Cisco License On-Prem: до 10-202609

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-09 / 2026-10-09

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ssm-Ph77wdhf
- https://bdu.fstec.ru/vul/2026-16101

153

Краткое описание: Получение конфиденциальной информации в Cisco Smart Software Manager On-Prem

Идентификатор уязвимости: CVE-2026-76483
BDU:2026-16102

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

Уязвимый продукт: Cisco Smart Software Manager On-Prem: до 10-202609
Cisco License On-Prem: до 10-202609

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-10-09 / 2026-10-09

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ssm-Ph77wdhf
- https://bdu.fstec.ru/vul/2026-16102