НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-01-17.1 | 17 января 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2024-6387	Dell PowerScale OneFS	Сетевой	ACE	2025-01-16	✓
2	Высокая	CVE-2024-52333	OFFIS DCMTK	Локальный	ACE	2025-01-16	✓
3	Высокая	CVE-2024-47796	OFFIS DCMTK	Локальный	ACE	2025-01-16	✓
4	Критическая	CVE-2024-12297	Moxa EDS-508A Series	Сетевой	OSI	2025-01-16	✓
5	Критическая	CVE-2024-41110	Dell OpenManage Network Integration (OMNI)	Сетевой	PE	2025-01-16	✓
6	Высокая	CVE-2024-6345	Dell OpenManage Network Integration (OMNI)	Сетевой	ACE	2025-01-16	✓
7	Высокая	CVE-2024-45490	Dell OpenManage Network Integration (OMNI)	Сетевой	ACE	2025-01-16	✓
8	Критическая	CVE-2024-45491	Dell OpenManage Network Integration (OMNI)	Сетевой	ACE	2025-01-16	✓
9	Критическая	CVE-2024-45492	Dell OpenManage Network Integration (OMNI)	Сетевой	ACE	2025-01-16	✓
10	Высокая	CVE-2024-10979	Dell OpenManage Network Integration (OMNI)	Сетевой	ACE	2025-01-16	✓
11	Критическая	CVE-2024-5171	Dell OpenManage Network Integration (OMNI)	Сетевой	ACE	2025-01-16	✓

12	Высокая	CVE-2024-46759	Dell OpenManage Network Integration (OMNI)	Локальный	ACE	2025-01-16	✓
13	Высокая	CVE-2024-46782	Dell OpenManage Network Integration (OMNI)	Локальный	PE	2025-01-16	✓
14	Высокая	CVE-2024-46798	Dell OpenManage Network Integration (OMNI)	Локальный	PE	2025-01-16	✓
15	Высокая	CVE-2024-46800	Dell OpenManage Network Integration (OMNI)	Локальный	PE	2025-01-16	✓
16	Высокая	CVE-2024-46744	Dell OpenManage Network Integration (OMNI)	Локальный	DoS	2025-01-16	✓
17	Высокая	CVE-2024-46740	Dell OpenManage Network Integration (OMNI)	Локальный	PE	2025-01-16	✓
18	Высокая	CVE-2024-46725	Dell OpenManage Network Integration (OMNI)	Локальный	DoS	2025-01-16	✓
19	Высокая	CVE-2024-46738	Dell OpenManage Network Integration (OMNI)	Локальный	PE	2025-01-16	✓
20	Высокая	CVE-2024-46804	Dell OpenManage Network Integration (OMNI)	Локальный	DoS	2025-01-16	✓
21	Высокая	CVE-2024-46815	Dell OpenManage Network Integration (OMNI)	Локальный	DoS	2025-01-16	✓
22	Критическая	CVE-2024-47606	Dell OpenManage Network Integration (OMNI)	Сетевой	ACE	2025-01-16	✓
23	Высокая	CVE-2024-46814	Dell OpenManage Network Integration (OMNI)	Локальный	DoS	2025-01-16	✓

24	Высокая	CVE-2024-46818	Dell OpenManage Network Integration (OMNI)	Локальный	DoS	2025-01-16	✓
25	Высокая	CVE-2024-46828	Dell OpenManage Network Integration (OMNI)	Локальный	DoS	2025-01-16	✓
26	Высокая	CVE-2024-46844	Dell OpenManage Network Integration (OMNI)	Локальный	DoS	2025-01-16	✓
27	Критическая	CVE-2024-32002	Dell OpenManage Network Integration (OMNI)	Сетевой	WLF	2025-01-16	✓
28	Высокая	CVE-2024-32004	Dell OpenManage Network Integration (OMNI)	Локальный	ACE	2025-01-16	✓
29	Высокая	CVE-2024-43858	Dell OpenManage Network Integration (OMNI)	Локальный	DoS	2025-01-16	✓
30	Высокая	CVE-2024-43839	Dell OpenManage Network Integration (OMNI)	Локальный	DoS	2025-01-16	✓
31	Высокая	CVE-2024-42301	Dell OpenManage Network Integration (OMNI)	Локальный	DoS	2025-01-16	✓
32	Высокая	CVE-2024-42302	Dell OpenManage Network Integration (OMNI)	Локальный	PE	2025-01-16	✓
33	Высокая	CVE-2025-20620	STEALTHONE D220/D340/D440	Сетевой	ACE	2025-01-16	✓
34	Критическая	CVE-2025-20055	STEALTHONE D220/D340/D440	Сетевой	ACE	2025-01-16	✓
35	Высокая	CVE-2024-42313	Dell OpenManage Network Integration (OMNI)	Локальный	PE	2025-01-16	✓

36	Высокая	CVE-2024-44998	Dell OpenManage Network Integration (OMNI)	Локальный	PE	2025-01-16	✓
37	Высокая	CVE-2024-46673	Dell OpenManage Network Integration (OMNI)	Локальный	PE	2025-01-16	✓
38	Высокая	CVE-2024-46674	Dell OpenManage Network Integration (OMNI)	Локальный	PE	2025-01-16	✓
39	Высокая	CVE-2024-44974	Dell OpenManage Network Integration (OMNI)	Локальный	PE	2025-01-16	✓
40	Высокая	CVE-2024-44987	Dell OpenManage Network Integration (OMNI)	Локальный	PE	2025-01-16	✓
41	Критическая	CVE-2024-50603	Aviatrix Controller	Сетевой	ACE	2025-01-13	✓
42	Критическая	CVE-2024-55591	FortiOS and FortiProxy	Сетевой	OSI	2025-01-14	✓
43	Критическая	CVE-2024-6516	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	XSS\CSS	2025-01-13	✓
44	Критическая	CVE-2024-6784	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	CSRF	2025-01-13	✓
45	Высокая	CVE-2024-48843	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	ACE	2025-01-13	✓
46	Критическая	CVE-2024-48839	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	ACE	2025-01-13	✓
47	Критическая	CVE-2024-48840	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	ACE	2025-01-13	✓

48	Высокая	CVE-2024-51541	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	OSI	2025-01-13	✓
49	Высокая	CVE-2024-51543	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	SB	2025-01-13	✓
50	Высокая	CVE-2024-51544	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	DoS	2025-01-13	✓
51	Критическая	CVE-2024-51548	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	WLF	2025-01-13	✓
52	Критическая	CVE-2024-51549	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	OAF	2025-01-13	✓
53	Критическая	CVE-2024-51550	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	ACE	2025-01-13	✓
54	Высокая	CVE-2024-11316	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	DoS	2025-01-13	✓
55	Высокая	CVE-2024-51546	ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products	Сетевой	OSI	2025-01-13	✓
56	Высокая	CVE-2024-7517	Brocade Fabric OS	Локальный	PE	2025-01-13	✓
57	Высокая	CVE-2022-1304	Brocade Fabric OS	Локальный	ACE	2025-01-13	✓
58	Критическая	CVE-2022-48624	Brocade Fabric OS	Сетевой	ACE	2025-01-13	✓
59	Высокая	CVE-2024-1086	Brocade Fabric OS	Локальный	ACE	2025-01-13	✓
60	Высокая	CVE-2025-0061	SAP BusinessObjects Business Intelligence suite	Сетевой	SB	2025-01-14	✓

61	Высокая	CVE-2025-21335	Microsoft Windows Hyper-V NT Kernel Integration VSP	Локальный	PE	2025-01-14	✓
62	Высокая	CVE-2025-21334	Microsoft Windows Hyper-V NT Kernel Integration VSP	Локальный	PE	2025-01-14	✓
63	Высокая	CVE-2025-21333	Microsoft Windows Hyper-V NT Kernel Integration VSP	Локальный	PE	2025-01-14	✓
64	Высокая	CVE-2025-21413	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
65	Высокая	CVE-2025-21409	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
66	Высокая	CVE-2025-21239	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
67	Высокая	CVE-2025-21339	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
68	Высокая	CVE-2025-21306	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
69	Высокая	CVE-2025-21243	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
70	Высокая	CVE-2025-21303	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
71	Высокая	CVE-2025-21417	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
72	Высокая	CVE-2025-21252	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
73	Высокая	CVE-2025-21273	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
74	Высокая	CVE-2025-21237	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓

75	Высокая	CVE-2025-21302	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
76	Высокая	CVE-2025-21250	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
77	Высокая	CVE-2025-21282	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
78	Высокая	CVE-2025-21241	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
79	Высокая	CVE-2025-21305	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
80	Высокая	CVE-2025-21223	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
81	Высокая	CVE-2025-21240	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
82	Высокая	CVE-2025-21411	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
83	Высокая	CVE-2025-21233	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
84	Высокая	CVE-2025-21286	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
85	Высокая	CVE-2025-21238	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
86	Высокая	CVE-2025-21248	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
87	Высокая	CVE-2025-21245	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
88	Высокая	CVE-2025-21236	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
89	Высокая	CVE-2025-21266	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓

90	Высокая	CVE-2025-21244	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
91	Высокая	CVE-2025-21246	Microsoft Windows Telephony Service	Сетевой	ACE	2025-01-14	✓
92	Высокая	CVE-2025-21402	Microsoft Office OneNote	Локальный	ACE	2025-01-14	✓
93	Высокая	CVE-2025-21291	Microsoft Windows Direct Show	Сетевой	ACE	2025-01-14	✓
94	Высокая	CVE-2025-21187	Microsoft Power Automate	Локальный	ACE	2025-01-14	✓
95	Высокая	CVE-2025-21344	Microsoft SharePoint Server	Локальный	ACE	2025-01-14	✓
96	Высокая	CVE-2025-21186	Microsoft Access	Локальный	ACE	2025-01-14	✓
97	Высокая	CVE-2025-21395	Microsoft Access	Локальный	ACE	2025-01-14	✓
98	Высокая	CVE-2025-21366	Microsoft Access	Локальный	ACE	2025-01-14	✓
99	Высокая	CVE-2025-21361	Microsoft Outlook	Локальный	ACE	2025-01-14	✓
100	Высокая	CVE-2025-21132	Adobe Substance 3D Stager	Локальный	ACE	2025-01-14	✓
101	Высокая	CVE-2025-21131	Adobe Substance 3D Stager	Локальный	ACE	2025-01-14	✓
102	Высокая	CVE-2025-21130	Adobe Substance 3D Stager	Локальный	ACE	2025-01-14	✓
103	Высокая	CVE-2025-21129	Adobe Substance 3D Stager	Локальный	ACE	2025-01-14	✓
104	Высокая	CVE-2025-21128	Adobe Substance 3D Stager	Локальный	ACE	2025-01-14	✓

105	Высокая	CVE-2025-21138	Adobe Substance 3D Designer	Локальный	ACE	2025-01-14	✓
106	Высокая	CVE-2025-21139	Adobe Substance 3D Designer	Локальный	ACE	2025-01-14	✓
107	Высокая	CVE-2025-21137	Adobe Substance 3D Designer	Локальный	ACE	2025-01-14	✓
108	Высокая	CVE-2025-21136	Adobe Substance 3D Designer	Локальный	ACE	2025-01-14	✓
109	Высокая	CVE-2025-21122	Adobe Photoshop	Локальный	ACE	2025-01-14	✓
110	Высокая	CVE-2025-21127	Adobe Photoshop	Локальный	ACE	2025-01-14	✓
111	Высокая	CVE-2025-21135	Adobe Animate	Локальный	ACE	2025-01-14	✓
112	Высокая	CVE-2025-21295	Microsoft SPNEGO Extended Negotiation (NEGOEX) Security Mechanism	Сетевой	ACE	2025-01-15	✓
113	Высокая	CVE-2025-21354	Microsoft Excel	Локальный	ACE	2025-01-15	✓
114	Высокая	CVE-2025-21364	Microsoft Excel	Локальный	ACE	2025-01-15	✓
115	Высокая	CVE-2025-21362	Microsoft Excel	Локальный	ACE	2025-01-15	✓
116	Высокая	CVE-2025-21365	Microsoft Office	Сетевой	ACE	2025-01-15	✓
117	Высокая	CVE-2025-21346	Microsoft Office	Сетевой	SB	2025-01-15	✓
118	Критическая	CVE-2025-21298	Microsoft Windows OLE	Сетевой	ACE	2025-01-15	✓
119	Высокая	CVE-2025-21178	Microsoft Visual Studio	Сетевой	ACE	2025-01-15	✓

120	Высокая	CVE-2025-21176	Microsoft .NET, .NET Framework, and Visual Studio	Сетевой	OSI	2025-01-15	✓
121	Критическая	CVE-2025-21307	Microsoft Windows Reliable Multicast Transport Driver (RMCAST)	Сетевой	ACE	2025-01-15	✓
122	Критическая	CVE-2025-21311	Microsoft Windows NTLM V1	Сетевой	PE	2025-01-15	✓
123	Высокая	CVE-2025-0442	Google Chrome	Сетевой	OSI	2025-01-15	✓
124	Высокая	CVE-2025-0441	Google Chrome	Сетевой	OSI	2025-01-15	✓
125	Высокая	CVE-2025-0440	Google Chrome	Сетевой	OSI	2025-01-15	✓
126	Высокая	CVE-2025-0439	Google Chrome	Сетевой	SB	2025-01-15	✓
127	Высокая	CVE-2025-0438	Google Chrome	Сетевой	ACE	2025-01-15	✓
128	Высокая	CVE-2025-0436	Google Chrome	Сетевой	ACE	2025-01-15	✓
129	Высокая	CVE-2025-0435	Google Chrome	Сетевой	OSI	2025-01-15	✓
130	Высокая	CVE-2025-0434	Google Chrome	Сетевой	ACE	2025-01-15	✓
131	Высокая	CVE-2025-21326	Microsoft Internet Explorer	Локальный	ACE	2025-01-15	✓
132	Высокая	CVE-2025-21363	Microsoft Word	Локальный	ACE	2025-01-15	✓
133	Высокая	CVE-2025-21345	Microsoft Office Visio	Локальный	ACE	2025-01-15	✓
134	Высокая	CVE-2025-21356	Microsoft Office Visio	Локальный	ACE	2025-01-15	✓

135	Высокая	CVE-2024-12085	Rsync	Сетевой	OSI	2025-01-14	✓
136	Критическая	CVE-2024-12084	Rsync	Сетевой	ACE	2025-01-14	✓
137	Высокая	CVE-2025-21297	Microsoft Windows Remote Desktop Services	Сетевой	ACE	2025-01-14	✓
138	Высокая	CVE-2025-21330	Microsoft Windows Remote Desktop Services	Сетевой	DoS	2025-01-14	✓
139	Высокая	CVE-2025-21309	Microsoft Windows Remote Desktop Services	Сетевой	ACE	2025-01-14	✓
140	Высокая	CVE-2025-21224	Microsoft Windows Line Printer Daemon (LPD) Service	Сетевой	ACE	2025-01-14	✓
141	Высокая	CVE-2025-21294	Microsoft Digest Authentication	Сетевой	ACE	2025-01-14	✓
142	Критическая	CVE-2023-34990	FortiWLM	Сетевой	RLF	2024-12-18	✓
143	Высокая	CVE-2024-48889	FortiManager	Сетевой	ACE	2024-12-18	✓
144	Критическая	CVE-2021-26102	FortiWAN	Сетевой	SB	2021-04-28	✓

1

Краткое описание: Выполнение произвольного кода в Dell PowerScale OneFS

Идентификатор уязвимости: CVE-2024-6387
BDU:2024-04914

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

Уязвимый продукт: PowerScale OneFS: до 9.4.0.19

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.openssh.com/releasenotes.html#9.8p1
- http://seclists.org/oss-sec/2024/q3/2
- https://bdu.fstec.ru/vul/2024-04914

2

Краткое описание: Выполнение произвольного кода в OFFIS DCMTK

Идентификатор уязвимости: CVE-2024-52333

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

Уязвимый продукт: DCMTK: 3.6.8

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.talosintelligence.com/vulnerability_reports/TALOS-2024-2121

3

Краткое описание: Выполнение произвольного кода в OFFIS DCMTK

Идентификатор уязвимости: CVE-2024-47796

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

Уязвимый продукт: DCMTK: 3.6.8

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.talosintelligence.com/vulnerability_reports/TALOS-2024-2122

4

Краткое описание: Получение конфиденциальной информации в Moxa EDS-508A Series

Идентификатор уязвимости: CVE-2024-12297

Идентификатор программной ошибки: CWE-656 Защитный механизм на основе неизвестности

Уязвимый продукт: EDS-508A: 3.11

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.moxa.com/en/support/product-support/security-advisory/mpsa-241407-cve-2024-12297-frontend-authorization-logic-disclosure-vulnerability-in-eds-508a-series

5

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-41110
BDU:2024-05760

Идентификатор программной ошибки: CWE-863 Некорректная авторизация

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-05760

6

Краткое описание: Выполнение произвольного кода в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-6345
BDU:2024-05843

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

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-05843

7

Краткое описание: Выполнение произвольного кода в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-45490
BDU:2024-07004

Идентификатор программной ошибки: CWE-124 Запись данных в область перед началом буфера

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных 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:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-07004

8

Краткое описание: Выполнение произвольного кода в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-45491
BDU:2024-07377

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

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-07377

9

Краткое описание: Выполнение произвольного кода в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-45492
BDU:2024-07376

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

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-07376

10

Краткое описание: Выполнение произвольного кода в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-10979
BDU:2024-09679

Идентификатор программной ошибки: CWE-285 Некорректная авторизация

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-09679

11

Краткое описание: Выполнение произвольного кода в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-5171
BDU:2024-04523

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

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-04523

12

Краткое описание: Выполнение произвольного кода в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46759
BDU:2024-08085

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

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08085

13

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46782
BDU:2024-08077

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08077

14

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46798
BDU:2024-08139

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08139

15

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46800
BDU:2024-08186

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08186

16

Краткое описание: Отказ в обслуживании в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46744
BDU:2024-08231

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08231

17

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46740
BDU:2024-08184

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08184

18

Краткое описание: Отказ в обслуживании в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46725
BDU:2024-08087

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08087

19

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46738
BDU:2024-08083

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08083

20

Краткое описание: Отказ в обслуживании в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46804
BDU:2024-08525

Идентификатор программной ошибки: CWE-399 Уязвимости, связанные с управлением ресурсами

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08525

21

Краткое описание: Отказ в обслуживании в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46815

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities

22

Краткое описание: Выполнение произвольного кода в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-47606

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

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities

23

Краткое описание: Отказ в обслуживании в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46814
BDU:2024-08528

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08528

24

Краткое описание: Отказ в обслуживании в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46818
BDU:2024-08529

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08529

25

Краткое описание: Отказ в обслуживании в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46828

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities

26

Краткое описание: Отказ в обслуживании в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46844
BDU:2024-08234

Идентификатор программной ошибки: CWE-682 Некорректные расчеты

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08234

27

Краткое описание: Запись локальных файлов в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-32002
BDU:2024-03872

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

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись локальных файлов

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-03872

28

Краткое описание: Выполнение произвольного кода в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-32004
BDU:2024-04093

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

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-04093

29

Краткое описание: Отказ в обслуживании в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-43858
BDU:2024-08533

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08533

30

Краткое описание: Отказ в обслуживании в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-43839

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities

31

Краткое описание: Отказ в обслуживании в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-42301
BDU:2024-08229

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08229

32

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-42302
BDU:2024-10086

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-10086

33

Краткое описание: Выполнение произвольного кода в STEALTHONE D220/D340/D440

Идентификатор уязвимости: CVE-2025-20620

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

Уязвимый продукт: STEALTHONE D220: 6.03.02
STEALTHONE D340: 6.03.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU99653331/index.html
- http://stealthone.net/product_info/d220-d340%e3%80%8cv6-03-03%e3%80%8d%e5%8f%8a%e3%81%b3d440%e3%80%8cv7-00-11

34

Краткое описание: Выполнение произвольного кода в STEALTHONE D220/D340/D440

Идентификатор уязвимости: CVE-2025-20055

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

Уязвимый продукт: STEALTHONE D220: 6.03.02
STEALTHONE D340: 6.03.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://jvn.jp/en/vu/JVNVU99653331/index.html
- http://stealthone.net/product_info/d220-d340%e3%80%8cv6-03-03%e3%80%8d%e5%8f%8a%e3%81%b3d440%e3%80%8cv7-00-11

35

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-42313
BDU:2024-09776

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-09776

36

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-44998
BDU:2024-06745

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-06745

37

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46673
BDU:2024-08531

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08531

38

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-46674
BDU:2024-08333

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-08333

39

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-44974
BDU:2024-06733

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-06733

40

Краткое описание: Повышение привилегий в Dell OpenManage Network Integration (OMNI)

Идентификатор уязвимости: CVE-2024-44987
BDU:2024-09526

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: OpenManage Network Integration (OMNI): до 3.7

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-16 / 2025-01-16

Ссылки на источник:

- http://www.dell.com/support/kbdoc/nl-nl/000272375/dsa-2025-035-security-update-for-dell-openmanage-network-integration-omni-vulnerabilities
- https://bdu.fstec.ru/vul/2024-09526

41

Краткое описание: Выполнение произвольного кода в Aviatrix Controller

Идентификатор уязвимости: CVE-2024-50603

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

Уязвимый продукт: Aviatrix Controller: с версии 7.0.1307 по 7.2.4820

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://docs.aviatrix.com/documentation/latest/release-notices/psirt-advisories/psirt-advisories.html?expand=true#remote-code-execution-vulnerability-in-aviatrix-controllers
- http://www.securing.pl/en/cve-2024-50603-aviatrix-network-controller-command-injection-vulnerability/
- http://www.wiz.io/blog/wiz-research-identifies-exploitation-in-the-wild-of-aviatrix-cve-2024-50603

Краткое описание: Получение конфиденциальной информации в FortiOS and FortiProxy

Идентификатор уязвимости: CVE-2024-55591
BDU:2025-00281

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

Уязвимый продукт: FortiOS: с версии 7.0.0 по 7.0.16
FortiProxy: с версии 7.0.0 по 7.2.99

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Получение конфиденциальной информации

42

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://www.fortiguard.com/psirt/FG-IR-24-535
- https://bdu.fstec.ru/vul/2025-00281

43

Краткое описание: Межсайтовый скриптинг в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-6516
BDU:2024-10880

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

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданной вредоносной ссылки.

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-10880

Краткое описание: Подделка запросов на стороне сервера в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-6784
BDU:2024-10925

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

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Подделка запросов на стороне сервера

44

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-10925

45

Краткое описание: Выполнение произвольного кода в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-48843
BDU:2024-10873

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

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.7 AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-10873

Краткое описание: Выполнение произвольного кода в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-48839
BDU:2024-11026

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

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

46

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-11026

Краткое описание: Выполнение произвольного кода в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-48840
BDU:2024-10892

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

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

47

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-10892

48

Краткое описание: Получение конфиденциальной информации в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-51541
BDU:2024-10871

Идентификатор программной ошибки: CWE-98 Уязвимости, связанные с именами файлов для PHP-функций include или require (удаленное внедрение файлов в PHP)

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-10871

Краткое описание: Обход безопасности в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-51543
BDU:2024-10870

Идентификатор программной ошибки: CWE-15 Возможность управления системой или настройками извне

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Обход безопасности

49

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-10870

Краткое описание: Отказ в обслуживании в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-51544
BDU:2024-10928

Идентификатор программной ошибки: CWE-15 Возможность управления системой или настройками извне

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Отказ в обслуживании

50

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-10928

Краткое описание: Запись локальных файлов в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-51548
BDU:2024-10869

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

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись локальных файлов

51

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-10869

Краткое описание: Перезапись произвольных файлов в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-51549
BDU:2024-10929

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

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Перезапись произвольных файлов

52

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-10929

Краткое описание: Выполнение произвольного кода в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-51550
BDU:2024-11025

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

53

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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:L

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-11025

Краткое описание: Отказ в обслуживании в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-11316
BDU:2024-10859

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

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

54

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-10859

Краткое описание: Получение конфиденциальной информации в ABB ASPECT-Enterprise, NEXUS, and MATRIX Series products

Идентификатор уязвимости: CVE-2024-51546
BDU:2024-10868

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: NEXUS-3: версии 3.08.02
NEX-2: версии 3.08.02
ASP-ENT: версии 3.08.02
MATRIX Series: версии 3.08.02

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Получение конфиденциальной информации

55

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://search.abb.com/library/Download.aspx?DocumentID=9AKK108469A7497&LanguageCode=en&DocumentPartId=&Action=Launch
- http://www.cisa.gov/news-events/ics-advisories/icsa-25-007-01
- https://bdu.fstec.ru/vul/2024-10868

Краткое описание: Повышение привилегий в Brocade Fabric OS

Идентификатор уязвимости: CVE-2024-7517
BDU:2024-10536

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

Уязвимый продукт: Brocade Fabric OS: с версии 9.2.0b1 по 9.2.1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Повышение привилегий

56

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04758en_us
- https://bdu.fstec.ru/vul/2024-10536

57

Краткое описание: Выполнение произвольного кода в Brocade Fabric OS

Идентификатор уязвимости: CVE-2022-1304
BDU:2022-03769

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Brocade Fabric OS: с версии 9.2.0b1 по 9.2.1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04758en_us
- https://bdu.fstec.ru/vul/2022-03769

58

Краткое описание: Выполнение произвольного кода в Brocade Fabric OS

Идентификатор уязвимости: CVE-2022-48624
BDU:2024-04438

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

Уязвимый продукт: Brocade Fabric OS: с версии 9.2.0b1 по 9.2.1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Некорректная проверка входных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04758en_us
- https://bdu.fstec.ru/vul/2024-04438

59

Краткое описание: Выполнение произвольного кода в Brocade Fabric OS

Идентификатор уязвимости: CVE-2024-1086
BDU:2024-01187

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Brocade Fabric OS: с версии 9.2.0b1 по 9.2.1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-13 / 2025-01-13

Ссылки на источник:

- http://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbst04758en_us
- https://bdu.fstec.ru/vul/2024-01187

60

Краткое описание: Обход безопасности в SAP BusinessObjects Business Intelligence suite

Идентификатор уязвимости: CVE-2025-0061

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: SAP BusinessObjects Business Intelligence suite: 4.2 - 2025

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://support.sap.com/en/my-support/knowledge-base/security-notes-news/january-2025.html
- http://me.sap.com/notes/3474398

61

Краткое описание: Повышение привилегий в Microsoft Windows Hyper-V NT Kernel Integration VSP

Идентификатор уязвимости: CVE-2025-21335
BDU:2025-00288

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2016 10.0.14393.7699, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2016 10.0.14393.7699, 2016 10.0.14393.7699

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21335
- https://bdu.fstec.ru/vul/2025-00288

62

Краткое описание: Повышение привилегий в Microsoft Windows Hyper-V NT Kernel Integration VSP

Идентификатор уязвимости: CVE-2025-21334
BDU:2025-00282

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2016 10.0.14393.7699, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2016 10.0.14393.7699, 2016 10.0.14393.7699

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21334
- https://bdu.fstec.ru/vul/2025-00282

63

Краткое описание: Повышение привилегий в Microsoft Windows Hyper-V NT Kernel Integration VSP

Идентификатор уязвимости: CVE-2025-21333
BDU:2025-00287

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2016 10.0.14393.7699, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2016 10.0.14393.7699, 2016 10.0.14393.7699

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Переполнение буфера.

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21333
- https://bdu.fstec.ru/vul/2025-00287

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21413

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

64 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21413

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21409

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

65

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21409

66

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21239
BDU:2025-00277

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2012 R2 6.3.9600.22371, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2012 R2 6.3.9600.22371, 2012 R2 6.3.9600.22371

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21239
- https://bdu.fstec.ru/vul/2025-00277

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21339

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

67 **Способ эксплуатации:** Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21339

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21306

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

68 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21306

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21243
BDU:2025-00279

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

69 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21243
- https://bdu.fstec.ru/vul/2025-00279

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21303

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

70 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21303

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21417

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

71 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21417

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21252

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

72 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21252

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21273

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

73 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21273

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21237
BDU:2025-00284

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

74 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21237
- https://bdu.fstec.ru/vul/2025-00284

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21302

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

75

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21302

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21250

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

76

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21250

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21282

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

77 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21282

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21241
BDU:2025-00280

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

78 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21241
- https://bdu.fstec.ru/vul/2025-00280

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21305

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

79 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21305

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21223
BDU:2025-00285

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

80 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21223
- https://bdu.fstec.ru/vul/2025-00285

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21240
BDU:2025-00283

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

81 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21240
- https://bdu.fstec.ru/vul/2025-00283

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21411

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

82

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21411

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21233
BDU:2025-00286

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

83 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21233
- https://bdu.fstec.ru/vul/2025-00286

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21286

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

84 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21286

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21238
BDU:2025-00276

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

85 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21238
- https://bdu.fstec.ru/vul/2025-00276

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21248

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

86

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21248

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21245

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

87 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21245

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21236
BDU:2025-00278

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

88 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21236
- https://bdu.fstec.ru/vul/2025-00278

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21266

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

89 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21266

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21244

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

90

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21244

Краткое описание: Выполнение произвольного кода в Microsoft Windows Telephony Service

Идентификатор уязвимости: CVE-2025-21246

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

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

91 **Способ эксплуатации:** Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21246

92

Краткое описание: Выполнение произвольного кода в Microsoft Office OneNote

Идентификатор уязвимости: CVE-2025-21402

Идентификатор программной ошибки: CWE-641 Некорректные ограничения для имен фалов и ресурсов

Уязвимый продукт: Microsoft OneNote for Mac: все версии
Microsoft Office LTSC: 2021 for Mac - 2024 for Mac

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21402

93

Краткое описание: Выполнение произвольного кода в Microsoft Windows Direct Show

Идентификатор уязвимости: CVE-2025-21291

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Windows: до версии 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до версии 2012 R2 6.3.9600.22371, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2012 R2 6.3.9600.22371

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21291

94

Краткое описание: Выполнение произвольного кода в Microsoft Power Automate

Идентификатор уязвимости: CVE-2025-21187

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

Уязвимый продукт: Power Automate for Desktop: все версии

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21187

95

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint Server

Идентификатор уязвимости: CVE-2025-21344

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft SharePoint Server: 2019
Microsoft SharePoint Server Subscription Edition: все версии
Microsoft SharePoint Enterprise Server: 2016

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21344

96

Краткое описание: Выполнение произвольного кода в Microsoft Access

Идентификатор уязвимости: CVE-2025-21186

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

Уязвимый продукт: Microsoft Office: 2019
Microsoft Access: 2016
Microsoft Office LTSC: 2021 - 2024
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21186

Краткое описание: Выполнение произвольного кода в Microsoft Access

Идентификатор уязвимости: CVE-2025-21395

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

Уязвимый продукт: Microsoft Office: 2019
Microsoft Access: 2016
Microsoft Office LTSC: 2021 - 2024
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

97

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21395

98

Краткое описание: Выполнение произвольного кода в Microsoft Access

Идентификатор уязвимости: CVE-2025-21366

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Office: 2019
Microsoft Access: 2016
Microsoft Office LTSC: 2021 - 2024
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21366

99

Краткое описание: Выполнение произвольного кода в Microsoft Outlook

Идентификатор уязвимости: CVE-2025-21361

Идентификатор программной ошибки: CWE-641 Некорректные ограничения для имен фалов и ресурсов

Уязвимый продукт: Microsoft Outlook for Mac: все версии
Microsoft Office LTSC: 2021 for Mac - 2024 for Mac

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21361

100

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

Идентификатор уязвимости: CVE-2025-21132

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Stager: с версии 1.0.0 по 3.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_stager/apsb25-03.html

101	**Краткое описание:** Выполнение произвольного кода в Adobe Substance 3D Stager **Идентификатор уязвимости:** CVE-2025-21131 **Идентификатор программной ошибки:** CWE-787 Запись за границами буфера **Уязвимый продукт:** Substance 3D Stager: с версии 1.0.0 по 3.0.4 **Категория уязвимого продукта:** Прикладное программное обеспечение **Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла. **Последствия эксплуатации:** Выполнение произвольного кода **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. **Оценка CVSSv3:** 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H **Вектор атаки:** Локальный **Взаимодействие с пользователем:** Требуется **Дата выявления / Дата обновления:** 2025-01-14 / 2025-01-14 **Ссылки на источник:** • http://helpx.adobe.com/security/products/substance3d_stager/apsb25-03.html

102	**Краткое описание:** Выполнение произвольного кода в Adobe Substance 3D Stager **Идентификатор уязвимости:** CVE-2025-21130 **Идентификатор программной ошибки:** CWE-787 Запись за границами буфера **Уязвимый продукт:** Substance 3D Stager: с версии 1.0.0 по 3.0.4 **Категория уязвимого продукта:** Прикладное программное обеспечение **Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла. **Последствия эксплуатации:** Выполнение произвольного кода **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. **Оценка CVSSv3:** 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H **Вектор атаки:** Локальный **Взаимодействие с пользователем:** Требуется **Дата выявления / Дата обновления:** 2025-01-14 / 2025-01-14 **Ссылки на источник:** • http://helpx.adobe.com/security/products/substance3d_stager/apsb25-03.html

103	**Краткое описание:** Выполнение произвольного кода в Adobe Substance 3D Stager **Идентификатор уязвимости:** CVE-2025-21129 **Идентификатор программной ошибки:** CWE-122 Переполнение буфера в динамической памяти **Уязвимый продукт:** Substance 3D Stager: с версии 1.0.0 по 3.0.4 **Категория уязвимого продукта:** Прикладное программное обеспечение **Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла. **Последствия эксплуатации:** Выполнение произвольного кода **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. **Оценка CVSSv3:** 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H **Вектор атаки:** Локальный **Взаимодействие с пользователем:** Требуется **Дата выявления / Дата обновления:** 2025-01-14 / 2025-01-14 **Ссылки на источник:** • http://helpx.adobe.com/security/products/substance3d_stager/apsb25-03.html

104	**Краткое описание:** Выполнение произвольного кода в Adobe Substance 3D Stager **Идентификатор уязвимости:** CVE-2025-21128 **Идентификатор программной ошибки:** CWE-121 Переполнение буфера в стеке **Уязвимый продукт:** Substance 3D Stager: с версии 1.0.0 по 3.0.4 **Категория уязвимого продукта:** Прикладное программное обеспечение **Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла. **Последствия эксплуатации:** Выполнение произвольного кода **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. **Оценка CVSSv3:** 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H **Вектор атаки:** Локальный **Взаимодействие с пользователем:** Требуется **Дата выявления / Дата обновления:** 2025-01-14 / 2025-01-14 **Ссылки на источник:** • http://helpx.adobe.com/security/products/substance3d_stager/apsb25-03.html

105

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

Идентификатор уязвимости: CVE-2025-21138

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Designer: с версии 5.0.0 по 14.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_designer/apsb25-06.html

106

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

Идентификатор уязвимости: CVE-2025-21139

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

Уязвимый продукт: Adobe Substance 3D Designer: с версии 5.0.0 по 14.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_designer/apsb25-06.html

107	**Краткое описание:** Выполнение произвольного кода в Adobe Substance 3D Designer **Идентификатор уязвимости:** CVE-2025-21137 **Идентификатор программной ошибки:** CWE-122 Переполнение буфера в динамической памяти **Уязвимый продукт:** Adobe Substance 3D Designer: с версии 5.0.0 по 14.0 **Категория уязвимого продукта:** Прикладное программное обеспечение **Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла. **Последствия эксплуатации:** Выполнение произвольного кода **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. **Оценка CVSSv3:** 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H **Вектор атаки:** Локальный **Взаимодействие с пользователем:** Требуется **Дата выявления / Дата обновления:** 2025-01-14 / 2025-01-14 **Ссылки на источник:** • http://helpx.adobe.com/security/products/substance3d_designer/apsb25-06.html

108

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

Идентификатор уязвимости: CVE-2025-21136

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Designer: с версии 5.0.0 по 14.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/substance3d_designer/apsb25-06.html

109

Краткое описание: Выполнение произвольного кода в Adobe Photoshop

Идентификатор уязвимости: CVE-2025-21122

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

Уязвимый продукт: Adobe Photoshop: с версии 25.0 по 26.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/photoshop/apsb25-02.html

110

Краткое описание: Выполнение произвольного кода в Adobe Photoshop

Идентификатор уязвимости: CVE-2025-21127

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: Adobe Photoshop: с версии 25.0 по 26.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://helpx.adobe.com/security/products/photoshop/apsb25-02.html

111	**Краткое описание:** Выполнение произвольного кода в Adobe Animate **Идентификатор уязвимости:** CVE-2025-21135 **Идентификатор программной ошибки:** CWE-191 Потеря значимости целых чисел (простой или циклический возврат) **Уязвимый продукт:** Animate: с версии 23.0.0 по 24.0.6 **Категория уязвимого продукта:** Прикладное программное обеспечение **Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла. **Последствия эксплуатации:** Выполнение произвольного кода **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В связи со сложившейся обстановкой и введенными санкциями против Российской Федерации рекомендуем устанавливать обновления программного обеспечения только после оценки всех сопутствующих рисков. **Оценка CVSSv3:** 7.8 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H **Вектор атаки:** Локальный **Взаимодействие с пользователем:** Требуется **Дата выявления / Дата обновления:** 2025-01-14 / 2025-01-14 **Ссылки на источник:** • http://helpx.adobe.com/security/products/animate/apsb25-05.html

112

Краткое описание: Выполнение произвольного кода в Microsoft SPNEGO Extended Negotiation (NEGOEX) Security Mechanism

Идентификатор уязвимости: CVE-2025-21295

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до 2008 R2 6.1.7601.27520, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21295

11
3

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-21354

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Office Online Server: все версии
Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024
Microsoft 365 Apps for Enterprise:
32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21354

11
4

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-21364

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Microsoft Office LTSC: 2024
Microsoft 365 Apps for Enterprise:
32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21364

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-21362

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Office Online Server: все версии
Microsoft Office: 2019
Microsoft Excel: 2016
Microsoft Office LTSC: 2021 - 2024
Microsoft 365 Apps for Enterprise:
32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

115

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21362

11
6

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2025-21365

Идентификатор программной ошибки: CWE-426 Подмена пути исполнения

Уязвимый продукт: Microsoft Office LTSC: 2024
Microsoft 365 Apps for Enterprise:
32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21365

117

Краткое описание: Обход безопасности в Microsoft Office

Идентификатор уязвимости: CVE-2025-21346

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Microsoft Office: 2016 - 2019
Microsoft Office LTSC: 2021 - 2024
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21346

11
8

Краткое описание: Выполнение произвольного кода в Microsoft Windows OLE

Идентификатор уязвимости: CVE-2025-21298

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21298
- http://www.zerodayinitiative.com/advisories/ZDI-25-028/

11
9

Краткое описание: Выполнение произвольного кода в Microsoft Visual Studio

Идентификатор уязвимости: CVE-2025-21178

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

Уязвимый продукт: Visual Studio: 16.0 - 2022 version 17.12

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21178

120

Краткое описание: Получение конфиденциальной информации в Microsoft .NET, .NET Framework, and Visual Studio

Идентификатор уязвимости: CVE-2025-21176

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Visual Studio: 16.0 - 2022 version 17.12
Microsoft .NET Framework: 3.5 - 4.8.1
.NET: 8.0.0 - 9.0

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21176

121

Краткое описание: Выполнение произвольного кода в Microsoft Windows Reliable Multicast Transport Driver (RMCAST)

Идентификатор уязвимости: CVE-2025-21307

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows: до 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21307

122

Краткое описание: Повышение привилегий в Microsoft Windows NTLM V1

Идентификатор уязвимости: CVE-2025-21311

Идентификатор программной ошибки: CWE-303 Некорректная реализация алгоритма аутентификации

Уязвимый продукт: Windows Server: до 2016 10.0.14393.7699, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2016 10.0.14393.7699, 2016 10.0.14393.7699

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Повышение привилегий

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21311

123

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2025-0442

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 131.0.6778.265

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_14.html
- http://crbug.com/40940854

124

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2025-0441

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 131.0.6778.265

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_14.html
- http://crbug.com/368628042

125

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2025-0440

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 131.0.6778.265

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Получение конфиденциальной информации

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

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_14.html
- http://crbug.com/40067914

126

Краткое описание: Обход безопасности в Google Chrome

Идентификатор уязвимости: CVE-2025-0439

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 131.0.6778.265

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Обход безопасности

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_14.html
- http://crbug.com/371247941

127

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2025-0438

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 131.0.6778.265

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_14.html
- http://crbug.com/384186539

128

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2025-0436

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 131.0.6778.265

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_14.html
- http://crbug.com/382786791

129

Краткое описание: Получение конфиденциальной информации в Google Chrome

Идентификатор уязвимости: CVE-2025-0435

Идентификатор программной ошибки: CWE-358 Некорректная реализация стандартизированных проверок безопасности

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 131.0.6778.265

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

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:H/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_14.html
- http://crbug.com/379652406

130

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2025-0434

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

Уязвимый продукт: Google Chrome: 100.0.4896.60 - 131.0.6778.265

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданной вредоносной веб-страницы.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://chromereleases.googleblog.com/2025/01/stable-channel-update-for-desktop_14.html
- http://crbug.com/374627491

131

Краткое описание: Выполнение произвольного кода в Microsoft Internet Explorer

Идентификатор уязвимости: CVE-2025-21326

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

Уязвимый продукт: Windows Server: до 2016 10.0.14393.7699, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2016 10.0.14393.7699, 2016 10.0.14393.7699

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21326

132

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2025-21363

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Microsoft Office LTSC: 2021 for Mac - 2024
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21363

133

Краткое описание: Выполнение произвольного кода в Microsoft Office Visio

Идентификатор уязвимости: CVE-2025-21345

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21345

134

Краткое описание: Выполнение произвольного кода в Microsoft Office Visio

Идентификатор уязвимости: CVE-2025-21356

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

Уязвимый продукт: Microsoft Office: 2019
Microsoft Office LTSC: 2021 - 2024
Microsoft 365 Apps for Enterprise: 32-bit Systems - 64-bit Systems

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-01-15 / 2025-01-15

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21356

135

Краткое описание: Получение конфиденциальной информации в Rsync

Идентификатор уязвимости: CVE-2024-12085

Идентификатор программной ошибки: CWE-457 Использование неинициализированной переменной

Уязвимый продукт: Rsync: 1.6.4 - 3.3.0pre1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://seclists.org/oss-sec/2025/q1/16

136

Краткое описание: Выполнение произвольного кода в Rsync

Идентификатор уязвимости: CVE-2024-12084

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

Уязвимый продукт: Rsync: 3.2.7 - 3.3.0pre1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных 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/E:U/RL:O/RC:C

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://seclists.org/oss-sec/2025/q1/16

13
7

Краткое описание: Выполнение произвольного кода в Microsoft Windows Remote Desktop Services

Идентификатор уязвимости: CVE-2025-21297

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows Server: до 2008 R2 6.1.7601.27520, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2019 10.0.17763.6775, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21297

138

Краткое описание: Отказ в обслуживании в Microsoft Windows Remote Desktop Services

Идентификатор уязвимости: CVE-2025-21330

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

Уязвимый продукт: Windows: до 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371 Windows Server: до 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2016 10.0.14393.7699, 2016 10.0.14393.7699

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21330

139

Краткое описание: Выполнение произвольного кода в Microsoft Windows Remote Desktop Services

Идентификатор уязвимости: CVE-2025-21309

Идентификатор программной ошибки: CWE-591 Хранение важных данных в некорректно заблокированной памяти

Уязвимый продукт: Windows Server: до 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2016 10.0.14393.7699, 2019 10.0.17763.6775, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2012 R2 6.3.9600.22371, 2012 R2 6.3.9600.22371, 2012 R2 6.3.9600.22371, 2012 R2 6.3.9600.22371

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21309

140

Краткое описание: Выполнение произвольного кода в Microsoft Windows Line Printer Daemon (LPD) Service

Идентификатор уязвимости: CVE-2025-21224

Идентификатор программной ошибки: CWE-591 Хранение важных данных в некорректно заблокированной памяти

Уязвимый продукт: Windows Server: до 2016 10.0.14393.7699, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2016 10.0.14393.7699, 2016 10.0.14393.7699
Windows: до 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21224

141

Краткое описание: Выполнение произвольного кода в Microsoft Digest Authentication

Идентификатор уязвимости: CVE-2025-21294

Идентификатор программной ошибки: CWE-591 Хранение важных данных в некорректно заблокированной памяти

Уязвимый продукт: Windows: до 10 21H2 10.0.19044.5371, 10 22H2 10.0.19045.5371, 10 1507 10.0.10240.20890, 10 1607 10.0.14393.7699, 10 1809 10.0.17763.6775, 11 22H2 10.0.22621.4751, 11 23H2 10.0.22631.4751, 11 24H2 10.0.26100.2894, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371, 10 21H2 10.0.19044.5371
Windows Server: до 2008 R2 6.1.7601.27520, 2008 6.0.6003.23070, 2012 R2 6.3.9600.22371, 2012 6.2.9200.25273, 2022 10.0.20348.3091, 2022 23H2 10.0.25398.1369, 2025 10.0.26100.2894, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520, 2008 R2 6.1.7601.27520

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-01-14 / 2025-01-14

Ссылки на источник:

- http://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-21294

142

Краткое описание: Чтение локальных файлов в FortiWLM

Идентификатор уязвимости: CVE-2023-34990
BDU:2024-11387

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

Уязвимый продукт: FortiWLM:
8.5.0 - 8.6.5

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Чтение локальных файлов

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-12-18 / 2024-12-18

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-23-144
- https://bdu.fstec.ru/vul/2024-11387

14
3

Краткое описание: Выполнение произвольного кода в FortiManager

Идентификатор уязвимости: CVE-2024-48889
BDU:2024-11467

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

Уязвимый продукт: FortiManager:
6.4.0 - 7.6.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Некорректная проверка входных 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: 7.2 AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-12-18 / 2024-12-18

Ссылки на источник:

- http://fortiguard.fortinet.com/psirt/FG-IR-24-425
- https://bdu.fstec.ru/vul/2024-11467

144

Краткое описание: Обход безопасности в FortiWAN

Идентификатор уязвимости: CVE-2021-26102
BDU:2021-02359

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: FortiWAN: до 5.1.1

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход процесса авторизации

Последствия эксплуатации: Обход безопасности

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2021-04-28 / 2021-04-28

Ссылки на источник:

- http://fortiguard.com/psirt/FG-IR-21-048
- https://bdu.fstec.ru/vul/2021-02359