НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-10-31.1 | 31 октября 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2025-55752	Apache Tomcat	Сетевой	ACE	2025-10-27	✓
2	Критическая	CVE-2025-55754	Apache Tomcat	Сетевой	ACE	2025-10-27	✓
3	Высокая	CVE-2025-59975	Juniper Networks Junos Space	Сетевой	DoS	2025-10-27	✓
4	Высокая	CVE-2025-10502	Google ChromeOS LTS	Сетевой	ACE	2025-10-24	✓
5	Высокая	CVE-2025-9133	Zyxel firewalls	Сетевой	OSI	2025-10-21	✓
6	Критическая	CVE-2024-35366	FFmpeg	Сетевой	ACE	2025-10-17	✓
7	Критическая	CVE-2024-35367	FFmpeg	Сетевой	OSI	2025-10-17	✓
8	Высокая	CVE-2025-40812	Siemens Solid Edge	Локальный	OSI	2025-10-16	✓
9	Высокая	CVE-2025-40811	Siemens Solid Edge	Локальный	OSI	2025-10-16	✓
10	Высокая	CVE-2025-40810	Siemens Solid Edge	Локальный	ACE	2025-10-16	✓
11	Высокая	CVE-2025-40809	Siemens Solid Edge	Локальный	ACE	2025-10-16	✓
12	Высокая	CVE-2025-59234	Microsoft Office	Локальный	ACE	2025-10-15	✓
13	Высокая	CVE-2025-59226	Microsoft Office Visio	Локальный	ACE	2025-10-15	✓

14	Высокая	CVE-2025-59222	Microsoft Word	Локальный	ACE	2025-10-15	✓
15	Высокая	CVE-2025-59225	Microsoft Excel	Локальный	ACE	2025-10-15	✓
16	Высокая	CVE-2025-59224	Microsoft Excel	Локальный	ACE	2025-10-15	✓
17	Высокая	CVE-2025-59223	Microsoft Excel	Локальный	ACE	2025-10-15	✓
18	Высокая	CVE-2025-59243	Microsoft Excel	Локальный	ACE	2025-10-15	✓
19	Высокая	CVE-2025-59236	Microsoft Excel	Локальный	ACE	2025-10-15	✓
20	Высокая	CVE-2025-59235	Microsoft Excel	Локальный	OSI	2025-10-15	✓
21	Высокая	CVE-2025-59233	Microsoft Excel	Локальный	ACE	2025-10-15	✓
22	Высокая	CVE-2025-59231	Microsoft Excel	Локальный	ACE	2025-10-15	✓
23	Высокая	CVE-2025-59238	Microsoft PowerPoint	Локальный	ACE	2025-10-15	✓
24	Критическая	CVE-2025-10230	Samba	Сетевой	ACE	2025-10-15	✓
25	Высокая	CVE-2025-59295	Microsoft Windows URL Parsing	Сетевой	ACE	2025-10-15	✓
26	Высокая	CVE-2025-55326	Microsoft Windows Connected Devices Platform Service (Cdpsvc)	Сетевой	ACE	2025-10-15	✓
27	Высокая	CVE-2025-58718	Microsoft Remote Desktop Client	Сетевой	ACE	2025-10-15	✓
28	Высокая	CVE-2025-57740	Fortinet products	Сетевой	ACE	2025-10-14	✓

29	Высокая	CVE-2025-11622	Ivanti Endpoint Manager (EPM)	Локальный	ACE	2025-10-14	✗
30	Высокая	CVE-2025-9713	Ivanti Endpoint Manager (EPM)	Сетевой	ACE	2025-10-14	✗
31	Высокая	CVE-2025-61804	Adobe Animate	Локальный	ACE	2025-10-14	✓
32	Высокая	CVE-2025-54279	Adobe Animate	Локальный	ACE	2025-10-14	✓
33	Высокая	CVE-2025-54268	Adobe Bridge	Локальный	ACE	2025-10-14	✓
34	Высокая	CVE-2025-61801	Adobe Dimension	Локальный	ACE	2025-10-14	✓
35	Высокая	CVE-2025-61800	Adobe Dimension	Локальный	ACE	2025-10-14	✓
36	Высокая	CVE-2025-61799	Adobe Dimension	Локальный	ACE	2025-10-14	✓
37	Высокая	CVE-2025-61798	Adobe Dimension	Локальный	ACE	2025-10-14	✓
38	Высокая	CVE-2025-54282	Adobe FrameMaker	Локальный	ACE	2025-10-14	✓
39	Высокая	CVE-2025-54281	Adobe FrameMaker	Локальный	ACE	2025-10-14	✓
40	Высокая	CVE-2025-54284	Adobe Illustrator	Локальный	ACE	2025-10-14	✓
41	Высокая	CVE-2025-54283	Adobe Illustrator	Локальный	ACE	2025-10-14	✓
42	Высокая	CVE-2025-54264	Adobe Commerce and Magento Open Source	Сетевой	XSS\CSS	2025-10-14	✓
43	Высокая	CVE-2025-54263	Adobe Commerce and Magento Open Source	Сетевой	OSI	2025-10-14	✓

44	Высокая	CVE-2025-54276	Adobe Substance 3D Modeler	Локальный	OSI	2025-10-14	✓
45	Высокая	CVE-2025-54280	Adobe Substance 3D Viewer	Локальный	ACE	2025-10-14	✓
46	Высокая	CVE-2025-54274	Adobe Substance 3D Viewer	Локальный	ACE	2025-10-14	✓
47	Высокая	CVE-2025-54273	Adobe Substance 3D Viewer	Локальный	ACE	2025-10-14	✓
48	Высокая	CVE-2025-61806	Adobe Substance 3D Stager	Локальный	OSI	2025-10-14	✓
49	Высокая	CVE-2025-61805	Adobe Substance 3D Stager	Локальный	OSI	2025-10-14	✓
50	Высокая	CVE-2025-61807	Adobe Substance 3D Stager	Локальный	ACE	2025-10-14	✓
51	Высокая	CVE-2025-61803	Adobe Substance 3D Stager	Локальный	ACE	2025-10-14	✓
52	Высокая	CVE-2025-61802	Adobe Substance 3D Stager	Локальный	ACE	2025-10-14	✓
53	Высокая	CVE-2025-59230	Microsoft Windows Remote Access Connection Manager	Локальный	ACE	2025-10-14	✓
54	Высокая	CVE-2025-24990	Microsoft Windows Agere Modem driver	Локальный	ACE	2025-10-14	✓
55	Критическая	CVE-2025-11719	Mozilla Firefox	Сетевой	DoS	2025-10-14	✓
56	Критическая	CVE-2025-11721	Mozilla Firefox	Сетевой	ACE	2025-10-14	✓
57	Высокая	CVE-2025-11720	Mozilla Firefox	Сетевой	SUI	2025-10-14	✓
58	Критическая	CVE-2025-11709	Mozilla Firefox	Сетевой	ACE	2025-10-14	✓

59	Критическая	CVE-2025-11710	Mozilla Firefox	Сетевой	OSI	2025-10-14	✓
60	Критическая	CVE-2025-11717	Mozilla Firefox	Сетевой	OSI	2025-10-14	✓
61	Критическая	CVE-2025-11708	Mozilla Firefox	Сетевой	ACE	2025-10-14	✓
62	Высокая	CVE-2025-11714	Mozilla Firefox	Сетевой	ACE	2025-10-14	✓
63	Высокая	CVE-2025-11715	Mozilla Firefox	Сетевой	ACE	2025-10-14	✓
64	Высокая	CVE-2025-11713	Mozilla Firefox	Сетевой	ACE	2025-10-14	✓
65	Высокая	CVE-2025-59968	Junos Space Security Director	Сетевой	OSI	2025-10-13	✓
66	Высокая	CVE-2025-59964	Juniper Junos OS	Сетевой	DoS	2025-10-13	✓
67	Высокая	CVE-2025-53645	Zimbra Collaboration	Сетевой	DoS	2025-10-06	✓

1

Краткое описание: Выполнение произвольного кода в Apache Tomcat

Идентификатор уязвимости: CVE-2025-55752

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

Уязвимый продукт: Apache Tomcat:
9.0.0 - 11.0.10

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 4.6 AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-27 / 2025-10-27

Ссылки на источник:

- https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.11
- https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.109
- https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.45

2

Краткое описание: Выполнение произвольного кода в Apache Tomcat

Идентификатор уязвимости: CVE-2025-55754

Идентификатор программной ошибки: CWE-117 Некорректная нейтрализация выходных данных для записи в журналы

Уязвимый продукт: Apache Tomcat:
9.0.0 - 11.0.10

Категория уязвимого продукта: Прикладное программное обеспечение

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

Оценка CVSSv4: 0.5 AV:N/AC:L/AT:P/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-27 / 2025-10-27

Ссылки на источник:

- https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.11
- https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.109
- https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.45

3

Краткое описание: Отказ в обслуживании в Juniper Networks Junos Space

Идентификатор уязвимости: CVE-2025-59975

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

Уязвимый продукт: Juniper Junos Space:
до 22.2R1 Patch V3

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-27 / 2025-10-27

Ссылки на источник:

- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-Space-Flooding-device-with-inbound-API-calls-leads-to-WebUI-and-CLI-management-access-DoS-CVE-2025-59975

4

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2025-10502
BDU:2025-11455

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

Уязвимый продукт: Chrome OS:
до 138.0.7204.295

Категория уязвимого продукта: Unix-подобные операционные системы 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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-24 / 2025-10-24

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/10/long-term-support-channel-update-for_23.html
- https://bdu.fstec.ru/vul/2025-11455

5

Краткое описание: Получение конфиденциальной информации в Zyxel firewalls

Идентификатор уязвимости: CVE-2025-9133

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: ATP series:
- - 5.40
USG FLEX series:
- - 5.40
USG FLEX 50W:
- - 5.40
USG20W-VPN:
- - 5.40

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Обход процесса авторизации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 6.2 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-21 / 2025-10-21

Ссылки на источник:

- https://www.zyxel.com/global/en/support/security-advisories/zyxel-security-advisory-for-post-authentication-command-injection-and-missing-authorization-vulnerabilities-in-zld-firewalls-10-21-2025

6

Краткое описание: Выполнение произвольного кода в FFmpeg

Идентификатор уязвимости: CVE-2024-35366
BDU:2025-00954

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

Уязвимый продукт: FFmpeg:
6.0 - 6.1.3

Категория уязвимого продукта: Прикладное программное обеспечение

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

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-17 / 2025-10-17

Ссылки на источник:

- https://gist.github.com/1047524396/1e72f170d58c2547ebd4db4cdf6cfabf
- https://github.com/FFmpeg/FFmpeg/blob/n6.1.1/libavformat/sbgdec.c#L389
- https://github.com/ffmpeg/ffmpeg/commit/0bed22d597b78999151e3bde0768b7fe763fc2a6
- https://bdu.fstec.ru/vul/2025-00954

7

Краткое описание: Получение конфиденциальной информации в FFmpeg

Идентификатор уязвимости: CVE-2024-35367
BDU:2025-06064

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: FFmpeg:
6.0 - 6.1.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Чтение за пределами буфера.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 2.7 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-17 / 2025-10-17

Ссылки на источник:

- https://gist.github.com/1047524396/9754a44845578358f6a403447c458ca4
- https://github.com/FFmpeg/FFmpeg/blob/n6.1.1/libavcodec/ppc/vp8dsp_altivec.c#L53
- https://github.com/ffmpeg/ffmpeg/commit/09e6840cf7a3ee07a73c3ae88a020bf27ca1a667
- https://bdu.fstec.ru/vul/2025-06064

8

Краткое описание: Получение конфиденциальной информации в Siemens Solid Edge

Идентификатор уязвимости: CVE-2025-40812

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Solid Edge:
до 224.0 Update 14

Категория уязвимого продукта: Прикладное программное обеспечение

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-16 / 2025-10-16

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-541582.html

9

Краткое описание: Получение конфиденциальной информации в Siemens Solid Edge

Идентификатор уязвимости: CVE-2025-40811

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Solid Edge:
до 224.0 Update 14

Категория уязвимого продукта: Прикладное программное обеспечение

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-16 / 2025-10-16

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-541582.html

10

Краткое описание: Выполнение произвольного кода в Siemens Solid Edge

Идентификатор уязвимости: CVE-2025-40810

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Solid Edge:
до 224.0 Update 14

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-16 / 2025-10-16

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-541582.html

11

Краткое описание: Выполнение произвольного кода в Siemens Solid Edge

Идентификатор уязвимости: CVE-2025-40809

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Solid Edge:
до 224.0 Update 14

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-16 / 2025-10-16

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-541582.html

12

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2025-59234
BDU:2025-13084

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59234
- https://bdu.fstec.ru/vul/2025-13084

13

Краткое описание: Выполнение произвольного кода в Microsoft Office Visio

Идентификатор уязвимости: CVE-2025-59226
BDU:2025-13074

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: 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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59226
- https://bdu.fstec.ru/vul/2025-13074

14

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2025-59222
BDU:2025-13093

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59222
- https://bdu.fstec.ru/vul/2025-13093

15

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-59225
BDU:2025-13044

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 for Mac
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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59225
- https://bdu.fstec.ru/vul/2025-13044

16

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-59224
BDU:2025-13075

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 for Mac
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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59224
- https://bdu.fstec.ru/vul/2025-13075

17

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-59223
BDU:2025-13043

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59223
- https://bdu.fstec.ru/vul/2025-13043

18

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-59243
BDU:2025-13014

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: 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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59243
- https://bdu.fstec.ru/vul/2025-13014

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-59236
BDU:2025-13013

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

19 **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: 8.4 AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: 8.1 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59236
- https://bdu.fstec.ru/vul/2025-13013

20

Краткое описание: Получение конфиденциальной информации в Microsoft Excel

Идентификатор уязвимости: CVE-2025-59235
BDU:2025-13086

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Office Online Server:
все версии
Microsoft SharePoint Server:
2019
Microsoft Office:
2019
Microsoft Excel:
2016
Microsoft Access:
2016
Microsoft Office LTSC:
2021 - 2024 for Mac
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: 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: 7.1 AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H

Оценка CVSSv4: 4.0 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59235
- https://bdu.fstec.ru/vul/2025-13086

21

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-59233
BDU:2025-13087

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

Уязвимый продукт: Office Online Server:
все версии
Microsoft Office:
2019
Microsoft Excel:
2016
Microsoft Office LTSC:
2021 - 2024 for Mac
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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59233
- https://bdu.fstec.ru/vul/2025-13087

22

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-59231
BDU:2025-13012

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

Уязвимый продукт: Office Online Server:
все версии
Microsoft Office:
2019
Microsoft Excel:
2016
Microsoft Office LTSC:
2021 - 2024 for Mac
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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59231
- https://bdu.fstec.ru/vul/2025-13012

23

Краткое описание: Выполнение произвольного кода в Microsoft PowerPoint

Идентификатор уязвимости: CVE-2025-59238
BDU:2025-13088

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Office:
2019
Microsoft PowerPoint:
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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59238
- https://bdu.fstec.ru/vul/2025-13088

Краткое описание: Выполнение произвольного кода в Samba

Идентификатор уязвимости: CVE-2025-10230
BDU:2025-13037

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

Уязвимый продукт: Samba:
4.0.0 - 4.23.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.8 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:P/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://www.samba.org/samba/security/CVE-2025-10230.html
- https://bdu.fstec.ru/vul/2025-13037

25

Краткое описание: Выполнение произвольного кода в Microsoft Windows URL Parsing

Идентификатор уязвимости: CVE-2025-59295
BDU:2025-13080

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

Уязвимый продукт: Windows Server:
2008 6.0.6003.22567 - 2025 10.0.26100.6584
Windows:
10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.6584

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Вызов пользователем специально созданной функции.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59295
- https://bdu.fstec.ru/vul/2025-13080

26

Краткое описание: Выполнение произвольного кода в Microsoft Windows Connected Devices Platform Service (Cdpsvc)

Идентификатор уязвимости: CVE-2025-55326
BDU:2025-13264

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows:
10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.6584
Windows Server:
2012 Gold - 2025 10.0.26100.6584

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

Оценка CVSSv4: 4.8 AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-55326
- https://bdu.fstec.ru/vul/2025-13264

27

Краткое описание: Выполнение произвольного кода в Microsoft Remote Desktop Client

Идентификатор уязвимости: CVE-2025-58718
BDU:2025-13277

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows Server:
2008 6.0.6003.22567 - 2025 10.0.26100.6584
Windows:
10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.6584

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-15 / 2025-10-15

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-58718
- https://bdu.fstec.ru/vul/2025-13277

Краткое описание: Выполнение произвольного кода в Fortinet products

Идентификатор уязвимости: CVE-2025-57740

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

Уязвимый продукт: FortiOS:
6.4.0 - 7.6.2
FortiPAM:
1.0.0 - 1.5.0
FortiProxy:
7.0.0 - 7.6.2

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

28 **Последствия эксплуатации:** Выполнение произвольного кода

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

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

Оценка CVSSv4: 5.2 AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-25-756

29

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager (EPM)

Идентификатор уязвимости: CVE-2025-11622

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Endpoint Manager:
2022 - 2024 SU3 Security Update 1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.3 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-October-2025?language=en_US&_gl=1*8qa97e*_gcl_au*MjAyOTA3ODYxOC4xNzYwNDc1MTQy

30

Краткое описание: Выполнение произвольного кода в Ivanti Endpoint Manager (EPM)

Идентификатор уязвимости: CVE-2025-9713
BDU:2025-12911

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

Уязвимый продукт: Endpoint Manager:
2022 - 2024 SU3 Security Update 1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-EPM-October-2025?language=en_US&_gl=1*8qa97e*_gcl_au*MjAyOTA3ODYxOC4xNzYwNDc1MTQy
- https://bdu.fstec.ru/vul/2025-12911

31

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2025-61804

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

Уязвимый продукт: Animate:
23.0.0 - 24.0.10

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/animate/apsb25-97.html

32

Краткое описание: Выполнение произвольного кода в Adobe Animate

Идентификатор уязвимости: CVE-2025-54279

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Animate:
23.0.0 - 24.0.10

Категория уязвимого продукта: Прикладное программное обеспечение

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:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/animate/apsb25-97.html

33

Краткое описание: Выполнение произвольного кода в Adobe Bridge

Идентификатор уязвимости: CVE-2025-54268

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

Уязвимый продукт: Adobe Bridge:
14.0.0 - 15.1.1

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/bridge/apsb25-96.html

34

Краткое описание: Выполнение произвольного кода в Adobe Dimension

Идентификатор уязвимости: CVE-2025-61801

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Dimension:
4.0.0 - 4.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

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:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/dimension/apsb25-103.html

35

Краткое описание: Выполнение произвольного кода в Adobe Dimension

Идентификатор уязвимости: CVE-2025-61800

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

Уязвимый продукт: Adobe Dimension:
4.0.0 - 4.1.4

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/dimension/apsb25-103.html

36

Краткое описание: Выполнение произвольного кода в Adobe Dimension

Идентификатор уязвимости: CVE-2025-61799

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe Dimension:
4.0.0 - 4.1.4

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/dimension/apsb25-103.html

37

Краткое описание: Выполнение произвольного кода в Adobe Dimension

Идентификатор уязвимости: CVE-2025-61798

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe Dimension:
4.0.0 - 4.1.4

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/dimension/apsb25-103.html

38

Краткое описание: Выполнение произвольного кода в Adobe FrameMaker

Идентификатор уязвимости: CVE-2025-54282

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

Уязвимый продукт: Adobe Framemaker:
2017.0 - 2022.7

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/framemaker/apsb25-101.html

39

Краткое описание: Выполнение произвольного кода в Adobe FrameMaker

Идентификатор уязвимости: CVE-2025-54281

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Adobe Framemaker:
2017.0 - 2022.7

Категория уязвимого продукта: Прикладное программное обеспечение

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:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/framemaker/apsb25-101.html

40

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2025-54284

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Illustrator:
28.0 - 29.6

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/illustrator/apsb25-102.html

41

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2025-54283

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Illustrator:
28.0 - 29.6

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/illustrator/apsb25-102.html

42

Краткое описание: Межсайтовый скриптинг в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2025-54264

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

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce):
2.4.4 - 2.4.9 alpha2
Adobe Commerce B2B:
1.3.3 - 1.5.3 alpha2
Magento Open Source:
2.4.4 - 2.4.9 alpha2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Внедрение HTML-кода.

Последствия эксплуатации: Межсайтовый скриптинг

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

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

Оценка CVSSv4: 1.0 AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/magento/apsb25-94.html

Краткое описание: Получение конфиденциальной информации в Adobe Commerce and Magento Open Source

Идентификатор уязвимости: CVE-2025-54263

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Adobe Commerce (formerly Magento Commerce):
2.4.4 - 2.4.9 alpha2
Adobe Commerce B2B:
1.3.3 - 1.5.3 alpha2
Magento Open Source:
2.4.4 - 2.4.9 alpha2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

43 **Последствия эксплуатации:** Получение конфиденциальной информации

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

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

Оценка CVSSv4: 6.3 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/magento/apsb25-94.html

44

Краткое описание: Получение конфиденциальной информации в Adobe Substance 3D Modeler

Идентификатор уязвимости: CVE-2025-54276

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe Substance 3D Modeler:
1.1 - 1.22.3

Категория уязвимого продукта: Прикладное программное обеспечение

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d-modeler/apsb25-100.html

45

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

Идентификатор уязвимости: CVE-2025-54280

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Viewer: 0.9.1 - 0.25.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-99.html

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

Идентификатор уязвимости: CVE-2025-54274

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Adobe Substance 3D Viewer:
0.9.1 - 0.25.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-99.html

47

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

Идентификатор уязвимости: CVE-2025-54273

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Viewer: 0.9.1 - 0.25.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-99.html

48

Краткое описание: Получение конфиденциальной информации в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2025-61806

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Substance 3D Stager:
1.0.0 - 3.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb25-104.html

49

Краткое описание: Получение конфиденциальной информации в Adobe Substance 3D Stager

Идентификатор уязвимости: CVE-2025-61805

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Substance 3D Stager:
1.0.0 - 3.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb25-104.html

50

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

Идентификатор уязвимости: CVE-2025-61807

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

Уязвимый продукт: Substance 3D Stager:
1.0.0 - 3.1.4

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb25-104.html

51

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

Идентификатор уязвимости: CVE-2025-61803

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

Уязвимый продукт: Substance 3D Stager:
1.0.0 - 3.1.4

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

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb25-104.html

52

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

Идентификатор уязвимости: CVE-2025-61802

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Substance 3D Stager:
1.0.0 - 3.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

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:N/UI:R/S:U/C:H/I:H/A:H

Оценка CVSSv4: 5.7 AV:L/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb25-104.html

Краткое описание: Выполнение произвольного кода в Microsoft Windows Remote Access Connection Manager

Идентификатор уязвимости: CVE-2025-59230
BDU:2025-12964

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Windows:
10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.6584
Windows Server:
2008 6.0.6003.22567 - 2025 10.0.26100.6584

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

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

Оценка CVSSv4: 8.5 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59230
- https://bdu.fstec.ru/vul/2025-12964

Краткое описание: Выполнение произвольного кода в Microsoft Windows Agere Modem driver

Идентификатор уязвимости: CVE-2025-24990
BDU:2025-12995

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Windows Server:
2008 6.0.6003.22567 - 2025 10.0.26100.6584
Windows:
10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.6584

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv4: 8.5 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-24990
- https://bdu.fstec.ru/vul/2025-12995

Краткое описание: Отказ в обслуживании в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-11719

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox:
143.0 - 143.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Отказ в обслуживании

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

55

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

Оценка CVSSv4: 1.2 AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-81/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1991950

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-11721

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

Уязвимый продукт: Mozilla Firefox:
143.0 - 143.0.4

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.

56

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-81/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1986816

Краткое описание: Пользовательский интерфейс подмены в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-11720

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

Уязвимый продукт: Firefox for Android:
140.0 - 143.0.4
Firefox Focus for Android:
до 144.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Пользовательский интерфейс подмены

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

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

Оценка CVSSv4: 1.2 AV:N/AC:L/AT:N/PR:N/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-81/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1979534
- https://bugzilla.mozilla.org/show_bug.cgi?id=1984370

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-11709

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Firefox ESR:
102.0 - 140.3.1
Mozilla Firefox:
100.0 - 143.0.4
Firefox for Android:
100.1.0 - 143.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-82/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-83/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-81/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1989127

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-11710

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

Уязвимый продукт: Firefox ESR:
102.0 - 140.3.1
Mozilla Firefox:
100.0 - 143.0.4
Firefox for Android:
100.1.0 - 143.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Оценка CVSSv4: 1.2 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-82/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-83/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-81/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1989899

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-11717

Идентификатор программной ошибки: CWE-1021 Некорректное ограничение отображаемых фреймов или слоев интерфейса

Уязвимый продукт: Firefox for Android:
140.0 - 143.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

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.

60

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

Оценка CVSSv4: 0.4 AV:P/AC:L/AT:N/PR:N/UI:A/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-81/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1872601

61

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-11708

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox:
120.0 - 143.0.4
Firefox ESR:
128.0 - 140.3.1
Firefox for Android:
120.0 - 143.0.4

Категория уязвимого продукта: Прикладное программное обеспечение

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

Оценка CVSSv4: 5.9 AV:N/AC:L/AT:N/PR:L/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-83/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-81/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1988931

62

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-11714

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

Уязвимый продукт: Firefox ESR:
102.0 - 140.3.1
Mozilla Firefox:
100.0 - 143.0.4
Firefox for Android:
100.1.0 - 143.0.4

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-82/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-83/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-81/
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1973699
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1989945
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1990970
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1991040

- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1992113

63

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-11715

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

Уязвимый продукт: Mozilla Firefox:
120.0 - 143.0.4
Firefox ESR:
128.0 - 140.3.1
Firefox for Android:
120.0 - 143.0.4

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

Оценка CVSSv4: 6.1 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-83/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-81/
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1983838
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1987624
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1988244
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1988912
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1989734

- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1990085
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1991899

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-11713

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

Уязвимый продукт: Mozilla Firefox:
120.0 - 143.0.4
Firefox ESR:
128.0 - 140.3.1

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 0.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N/E:U

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-10-14 / 2025-10-14

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-83/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-81/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1986142

Краткое описание: Получение конфиденциальной информации в Junos Space Security Director

Идентификатор уязвимости: CVE-2025-59968

Идентификатор программной ошибки: CWE-862 Отсутствие авторизации

Уязвимый продукт: Junos Space Security Director:
до 24.1R3 Patch V4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса авторизации

Последствия эксплуатации: Получение конфиденциальной информации

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

65

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

Оценка CVSSv4: 4.4 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:H/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-13 / 2025-10-13

Ссылки на источник:

- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Juniper-Security-Director-Insufficient-authorization-for-sensitive-resources-in-web-interface-CVE-2025-59968

66

Краткое описание: Отказ в обслуживании в Juniper Junos OS

Идентификатор уязвимости: CVE-2025-59964

Идентификатор программной ошибки: CWE-908 Использование неинициализированных ресурсов

Уязвимый продукт: Juniper Junos OS:
до 24.4R1-S3, 24.4R2

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Оценка CVSSv4: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-13 / 2025-10-13

Ссылки на источник:

- https://supportportal.juniper.net/s/article/2025-10-Security-Bulletin-Junos-OS-SRX4700-When-forwarding-options-sampling-is-enabled-any-traffic-destined-to-the-RE-will-cause-the-forwarding-line-card-to-crash-and-restart-CVE-2025-59964

Краткое описание: Отказ в обслуживании в Zimbra Collaboration

Идентификатор уязвимости: CVE-2025-53645

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Zimbra Collaboration:
9.0.0 - 10.1.8

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Отказ в обслуживании

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

67

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

Оценка CVSSv4: 6.6 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-06 / 2025-10-06

Ссылки на источник:

- https://wiki.zimbra.com/wiki/Security_Center#ZCS_9.0.0_Patch_46_Released
- https://wiki.zimbra.com/wiki/Security_Center#ZCS_10.0.15_Released
- https://wiki.zimbra.com/wiki/Security_Center#ZCS_10.1.9_Released