НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-12-15.1 | 15 декабря 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2025-54496	Fuji Electric Monitouch V-SFT	Локальный	ACE	2025-12-12	✓
2	Высокая	CVE-2025-54526	Fuji Electric Monitouch V-SFT	Локальный	ACE	2025-12-12	✓
3	Высокая	CVE-2025-26866	Apache HugeGraph-Server	Сетевой	ACE	2025-12-11	✓
4	Высокая	CVE-2025-64783	Adobe DNG Software Development Kit	Локальный	ACE	2025-12-10	✓
5	Высокая	CVE-2025-61813	Adobe ColdFusion	Сетевой	OSI	2025-12-10	✓
6	Высокая	CVE-2025-61812	Adobe ColdFusion	Смежная сеть	ACE	2025-12-10	✓
7	Высокая	CVE-2025-61811	Adobe ColdFusion	Сетевой	OSI	2025-12-10	✓
8	Высокая	CVE-2025-61810	Adobe ColdFusion	Сетевой	ACE	2025-12-10	✓
9	Критическая	CVE-2025-61809	Adobe ColdFusion	Сетевой	ACE	2025-12-10	✓
10	Критическая	CVE-2025-61808	Adobe ColdFusion	Сетевой	WLF	2025-12-10	✓
11	Высокая	CVE-2025-64899	Adobe Acrobat and Reader	Локальный	OSI	2025-12-09	✓
12	Высокая	CVE-2025-64785	Adobe Acrobat and Reader	Локальный	ACE	2025-12-09	✓
13	Высокая	CVE-2025-64671	GitHub Copilot for Jetbrains	Локальный	ACE	2025-12-09	✓

14	Высокая	CVE-2025-54100	Microsoft PowerShell	Локальный	ACE	2025-12-09	✓
15	Высокая	CVE-2025-62558	Microsoft Word	Локальный	ACE	2025-12-09	✓
16	Высокая	CVE-2025-62559	Microsoft Word	Локальный	ACE	2025-12-09	✓
17	Высокая	CVE-2025-62557	Microsoft Office	Локальный	ACE	2025-12-09	✓
18	Высокая	CVE-2025-62554	Microsoft Office	Локальный	ACE	2025-12-09	✓
19	Высокая	CVE-2025-62562	Microsoft Outlook	Локальный	ACE	2025-12-09	✓
20	Высокая	CVE-2025-62563	Microsoft Excel	Локальный	ACE	2025-12-09	✓
21	Высокая	CVE-2025-62564	Microsoft Excel	Локальный	OSI	2025-12-09	✓
22	Высокая	CVE-2025-62553	Microsoft Excel	Локальный	ACE	2025-12-09	✓
23	Высокая	CVE-2025-62556	Microsoft Excel	Локальный	ACE	2025-12-09	✓
24	Высокая	CVE-2025-62560	Microsoft Excel	Локальный	ACE	2025-12-09	✓
25	Высокая	CVE-2025-62561	Microsoft Excel	Локальный	ACE	2025-12-09	✓
26	Высокая	CVE-2025-62552	Microsoft Access	Локальный	WLF	2025-12-09	✓
27	Высокая	CVE-2025-62549	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2025-12-09	✓
28	Высокая	CVE-2025-64678	Microsoft Windows Routing and Remote Access Service (RRAS)	Сетевой	ACE	2025-12-09	✓

29	Высокая	CVE-2025-64447	FortiWeb	Сетевой	ACE	2025-12-09	✓
30	Высокая	CVE-2025-62221	Microsoft Windows Cloud Files Mini Filter driver	Локальный	ACE	2025-12-09	✓
31	Высокая	CVE-2025-13662	Ivanti Endpoint Manager (EPM)	Локальный	ACE	2025-12-09	✓
32	Высокая	CVE-2025-13659	Ivanti Endpoint Manager (EPM)	Сетевой	ACE	2025-12-09	✓
33	Критическая	CVE-2025-10573	Ivanti Endpoint Manager (EPM)	Сетевой	XSS\CSS	2025-12-09	✓
34	Высокая	CVE-2025-14327	Mozilla Firefox	Сетевой	OSI	2025-12-09	✓
35	Критическая	CVE-2025-14326	Mozilla Firefox	Сетевой	SB	2025-12-09	✓
36	Высокая	CVE-2025-14333	Mozilla Firefox	Сетевой	ACE	2025-12-09	✓
37	Критическая	CVE-2025-14330	Mozilla Firefox	Сетевой	SB	2025-12-09	✓
38	Высокая	CVE-2025-14329	Mozilla Firefox	Сетевой	SB	2025-12-09	✓
39	Высокая	CVE-2025-14328	Mozilla Firefox	Сетевой	SB	2025-12-09	✓
40	Критическая	CVE-2025-14324	Mozilla Firefox	Сетевой	ACE	2025-12-09	✓
41	Высокая	CVE-2025-14323	Mozilla Firefox	Сетевой	SB	2025-12-09	✓
42	Высокая	CVE-2025-14322	Mozilla Firefox	Сетевой	OSI	2025-12-09	✓
43	Критическая	CVE-2025-14321	Mozilla Firefox	Сетевой	ACE	2025-12-09	✓

44	Высокая	CVE-2025-53843	FortiOS	Сетевой	ACE	2025-11-18	✓
45	Высокая	CVE-2025-20349	Cisco Catalyst Center	Сетевой	PE	2025-11-13	✓

1

Краткое описание: Выполнение произвольного кода в Fuji Electric Monitouch V-SFT

Идентификатор уязвимости: CVE-2025-54496

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

Уязвимый продукт: Monitouch V-SFT:
6.2.7.0

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

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: 2025-12-12 / 2025-12-12

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1062/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-308-01
- https://www.zerodayinitiative.com/advisories/ZDI-25-1065/
- https://www.zerodayinitiative.com/advisories/ZDI-25-1068/

2

Краткое описание: Выполнение произвольного кода в Fuji Electric Monitouch V-SFT

Идентификатор уязвимости: CVE-2025-54526

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Monitouch V-SFT:
6.2.7.0

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

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: 2025-12-12 / 2025-12-12

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1063/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-308-01
- https://www.zerodayinitiative.com/advisories/ZDI-25-1064/
- https://www.zerodayinitiative.com/advisories/ZDI-25-1067/
- https://www.zerodayinitiative.com/advisories/ZDI-25-1066/

3

Краткое описание: Выполнение произвольного кода в Apache HugeGraph-Server

Идентификатор уязвимости: CVE-2025-26866

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

Уязвимый продукт: HugeGraph-Server:
1.0.0 - 1.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/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: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-11 / 2025-12-11

Ссылки на источник:

- https://lists.apache.org/thread/sd39g2bpo6pyohpy31z678p990sxoonh

4

Краткое описание: Выполнение произвольного кода в Adobe DNG Software Development Kit

Идентификатор уязвимости: CVE-2025-64783

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

Уязвимый продукт: Adobe DNG Software Development Kit (SDK): до 1.7.1

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: 2025-12-10 / 2025-12-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/dng-sdk/apsb25-118.html

5

Краткое описание: Получение конфиденциальной информации в Adobe ColdFusion

Идентификатор уязвимости: CVE-2025-61813

Идентификатор программной ошибки: CWE-611 Некорректное ограничение ссылок на внешние сущности XML

Уязвимый продукт: ColdFusion:
2021 - 2025 Update 4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-12-10 / 2025-12-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb25-105.html

6

Краткое описание: Выполнение произвольного кода в Adobe ColdFusion

Идентификатор уязвимости: CVE-2025-61812

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: ColdFusion:
2021 - 2025 Update 4

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

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

Вектор атаки: Смежная сеть

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-10 / 2025-12-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb25-105.html

7

Краткое описание: Получение конфиденциальной информации в Adobe ColdFusion

Идентификатор уязвимости: CVE-2025-61811

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: ColdFusion:
2021 - 2025 Update 4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-12-10 / 2025-12-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb25-105.html

8

Краткое описание: Выполнение произвольного кода в Adobe ColdFusion

Идентификатор уязвимости: CVE-2025-61810

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: ColdFusion:
2021 - 2025 Update 4

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-12-10 / 2025-12-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb25-105.html

9

Краткое описание: Выполнение произвольного кода в Adobe ColdFusion

Идентификатор уязвимости: CVE-2025-61809

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: ColdFusion:
2021 - 2025 Update 4

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:H/I:H/A:N

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-10 / 2025-12-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb25-105.html

10

Краткое описание: Запись локальных файлов в Adobe ColdFusion

Идентификатор уязвимости: CVE-2025-61808

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

Уязвимый продукт: ColdFusion:
2021 - 2025 Update 4

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-10 / 2025-12-10

Ссылки на источник:

- https://helpx.adobe.com/security/products/coldfusion/apsb25-105.html

Краткое описание: Получение конфиденциальной информации в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2025-64899

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Adobe Acrobat:
20.001.30002 - 2025.011.2
Adobe Reader:
20.001.30002 - 25.001.20982

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

11 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. В 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: 1.0 AV:L/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: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb25-119.html
- https://www.zerodayinitiative.com/advisories/ZDI-25-1043/

Краткое описание: Выполнение произвольного кода в Adobe Acrobat and Reader

Идентификатор уязвимости: CVE-2025-64785

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: Adobe Acrobat:
20.001.30002 - 2025.011.2
Adobe Reader:
20.001.30002 - 25.001.20982

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

12

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В 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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://helpx.adobe.com/security/products/acrobat/apsb25-119.html

Краткое описание: Выполнение произвольного кода в GitHub Copilot for Jetbrains

Идентификатор уязвимости: CVE-2025-64671

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: GitHub Copilot:
все версии

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

13 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-64671

Краткое описание: Выполнение произвольного кода в Microsoft PowerShell

Идентификатор уязвимости: CVE-2025-54100

Идентификатор программной ошибки: CWE-77 Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)

Уязвимый продукт: Windows:
10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.7392
Windows Server:
2008 6.0.6003.22567 - 2025 10.0.26100.7392

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

14

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В 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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-54100

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2025-62558

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

15

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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62558

16

Краткое описание: Выполнение произвольного кода в Microsoft Word

Идентификатор уязвимости: CVE-2025-62559

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft SharePoint Server:
2019
Microsoft Office:
2019
Microsoft Word:
2016
Microsoft SharePoint Enterprise Server:
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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62559

17

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2025-62557

Идентификатор программной ошибки: CWE-416 Использование после освобождения

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

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: 8.4 AV:L/AC:L/PR:N/UI:N/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: Отсутствует

Дата выявления / Дата обновления: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62557

Краткое описание: Выполнение произвольного кода в Microsoft Office

Идентификатор уязвимости: CVE-2025-62554

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

Уязвимый продукт: Microsoft Office LTSC:
2021 - 2024 for Mac
Microsoft Office:
2016 - 2019
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

18 **Способ эксплуатации:** Открытие пользователем специально созданной вредоносной ссылки.

Последствия эксплуатации: Выполнение произвольного кода

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

Дата выявления / Дата обновления: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62554

19

Краткое описание: Выполнение произвольного кода в Microsoft Outlook

Идентификатор уязвимости: CVE-2025-62562

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft SharePoint Server:
2019
Microsoft Office:
2019
Microsoft Word:
2016
Microsoft SharePoint Enterprise Server:
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: 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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62562

20

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-62563

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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62563

21

Краткое описание: Получение конфиденциальной информации в Microsoft Excel

Идентификатор уязвимости: CVE-2025-62564

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

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: 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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62564

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-62553

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: 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

22 **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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62553

23

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-62556

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62556

24

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-62560

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62560

25

Краткое описание: Выполнение произвольного кода в Microsoft Excel

Идентификатор уязвимости: CVE-2025-62561

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62561

Краткое описание: Запись локальных файлов в Microsoft Access

Идентификатор уязвимости: CVE-2025-62552

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

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

26 **Способ эксплуатации:** Открытие пользователем 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: 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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62552

27

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2025-62549

Идентификатор программной ошибки: CWE-822 Разыменование непроверенного указателя

Уязвимый продукт: Windows:
10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.7171
Windows Server:
2008 6.0.6003.22567 - 2025 10.0.26100.7171

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка пользователем запроса 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

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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62549

28

Краткое описание: Выполнение произвольного кода в Microsoft Windows Routing and Remote Access Service (RRAS)

Идентификатор уязвимости: CVE-2025-64678

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

Уязвимый продукт: Windows:
10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.6899
Windows Server:
2008 6.0.6003.22567 - 2025 10.0.26100.6899

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка пользователем запроса 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

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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-64678

29

Краткое описание: Выполнение произвольного кода в FortiWeb

Идентификатор уязвимости: CVE-2025-64447

Идентификатор программной ошибки: CWE-565 Использование куки-файлов без подтверждения и проверки целостности

Уязвимый продукт: FortiWeb:
7.0.0 - 8.0.1

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 7.2 AV:N/AC:H/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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-25-945

Краткое описание: Выполнение произвольного кода в Microsoft Windows Cloud Files Mini Filter driver

Идентификатор уязвимости: CVE-2025-62221

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Windows:
10 21H2 10.0.19041.3920 - 11 24H2 10.0.26100.7171
Windows Server:
2008 R2 - 2025 10.0.26100.7171

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

30

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. В 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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-62221

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

Идентификатор уязвимости: CVE-2025-13662

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: Endpoint Manager:
2022 - 2024 SU4

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.

31

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://forums.ivanti.com/s/article/Security-Advisory-EPM-December-2025-for-EPM-2024?language=en_US&_gl=1*1enaa74*_gcl_au*NDAxNzU2MDQxLjE3NjUzMDE2MTA.

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

Идентификатор уязвимости: CVE-2025-13659

Идентификатор программной ошибки: CWE-913 Некорректное управление динамически изменяемыми программными ресурсами

Уязвимый продукт: Endpoint Manager:
2022 - 2024 SU4

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.

32

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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://forums.ivanti.com/s/article/Security-Advisory-EPM-December-2025-for-EPM-2024?language=en_US&_gl=1*1enaa74*_gcl_au*NDAxNzU2MDQxLjE3NjUzMDE2MTA.

33

Краткое описание: Межсайтовый скриптинг в Ivanti Endpoint Manager (EPM)

Идентификатор уязвимости: CVE-2025-10573

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

Уязвимый продукт: Endpoint Manager:
2022 - 2024 SU4

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

Оценка CVSSv4: 4.9 AV:N/AC:L/AT:N/PR:N/UI:P/VC:H/VI:N/VA:N/SC:L/SI:L/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://forums.ivanti.com/s/article/Security-Advisory-EPM-December-2025-for-EPM-2024?language=en_US&_gl=1*1enaa74*_gcl_au*NDAxNzU2MDQxLjE3NjUzMDE2MTA.

34

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-14327

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

Уязвимый продукт: Mozilla Firefox:
141.0 - 145.0.2
Firefox for Android:
141.0 - 145.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

Дата выявления / Дата обновления: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-92/

Краткое описание: Обход безопасности в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-14326

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox:
141.0 - 145.0.2
Firefox for Android:
141.0 - 145.0.2

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Обход безопасности

35

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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:L/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-92/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-14333

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

Уязвимый продукт: Mozilla Firefox:
120.0 - 145.0.2
Firefox for Android:
120.0 - 145.0.2
Firefox ESR:
128.0 - 140.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

36

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-94/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-92/

Краткое описание: Обход безопасности в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-14330

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Mozilla Firefox:
120.0 - 145.0.2
Firefox for Android:
120.0 - 145.0.2
Firefox ESR:
128.0 - 140.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

37

Последствия эксплуатации: Обход безопасности

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-94/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-92/

Краткое описание: Обход безопасности в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-14329

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Mozilla Firefox:
120.0 - 145.0.2
Firefox for Android:
120.0 - 145.0.2
Firefox ESR:
128.0 - 140.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

38

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: 1.2 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-94/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-92/

Краткое описание: Обход безопасности в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-14328

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Mozilla Firefox:
120.0 - 145.0.2
Firefox for Android:
120.0 - 145.0.2
Firefox ESR:
128.0 - 140.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

39

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: 1.2 AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-94/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-92/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-14324

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Mozilla Firefox:
100.0 - 145.0.2
Firefox for Android:
100.1.0 - 145.0.2
Firefox ESR:
102.0 - 140.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

40

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

Оценка CVSSv3: 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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-93/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-94/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-92/

41

Краткое описание: Обход безопасности в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-14323

Идентификатор программной ошибки: CWE-269 Некорректное управление привилегиями

Уязвимый продукт: Mozilla Firefox:
100.0 - 145.0.2
Firefox for Android:
100.1.0 - 145.0.2
Firefox ESR:
102.0 - 140.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-93/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-94/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-92/

Краткое описание: Получение конфиденциальной информации в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-14322

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

Уязвимый продукт: Mozilla Firefox:
100.0 - 145.0.2
Firefox for Android:
100.1.0 - 145.0.2
Firefox ESR:
102.0 - 140.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-93/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-94/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-92/

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-14321

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox:
120.0 - 145.0.2
Firefox for Android:
120.0 - 145.0.2
Firefox ESR:
128.0 - 140.5.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

43

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2025-12-09 / 2025-12-09

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-94/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-92/

Краткое описание: Выполнение произвольного кода в FortiOS

Идентификатор уязвимости: CVE-2025-53843

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

Уязвимый продукт: FortiOS:
6.4.0 - 7.6.3

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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: 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:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-18 / 2025-11-18

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-25-358

45

Краткое описание: Повышение привилегий в Cisco Catalyst Center

Идентификатор уязвимости: CVE-2025-20349

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

Уязвимый продукт: Cisco DNA Center (Catalyst Center):
2.1.2.0 - 2.3.7.9

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: 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: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-11-13 / 2025-11-13

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-ci-ZWLQVSwT
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwo77762