НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-09-08.1 | 8 сентября 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2025-20134	Cisco ASA and FTD	Сетевой	DoS	2025-08-19	✓
2	Высокая	CVE-2025-20148	Cisco Secure Firewall Management Center (FMC)	Сетевой	CSRF	2025-08-15	✓
3	Высокая	CVE-2025-20217	Cisco Secure Firewall Management Center (FMC) and Firepower Threat Defense (FTD)	Сетевой	DoS	2025-08-15	✓
4	Высокая	CVE-2025-20222	Cisco ASA and FTD IPv6 over IPsec feature	Сетевой	DoS	2025-08-14	✓
5	Высокая	CVE-2025-9478	Google Chrome	Сетевой	ACE	2025-08-27	✓
6	Высокая	CVE-2025-47273	Ansible Automation Platform 2.5 packages	Сетевой	ACE	2025-08-26	✓
7	Высокая	CVE-2025-27819	Apache Kafka	Сетевой	DoS	2025-08-26	✓
8	Высокая	CVE-2025-6377	Rockwell Automation Arena	Локальный	ACE	2025-08-25	✓
9	Высокая	CVE-2025-6376	Rockwell Automation Arena	Локальный	ACE	2025-08-25	✓
10	Высокая	CVE-2025-9185	Mozilla Thunderbird 140.x, Thunderbird ESR и Thunderbird	Сетевой	SB	2025-08-23	✓
11	Высокая	CVE-2025-9184	Mozilla Thunderbird 140.x и Thunderbird	Сетевой	ACE	2025-08-23	✓

12	Высокая	CVE-2025-9182	Mozilla Thunderbird 140.x и Thunderbird	Сетевой	DoS	2025-08-23	✓
13	Высокая	CVE-2025-9180	Mozilla Thunderbird 140.x, Thunderbird ESR и Thunderbird	Сетевой	ACE	2025-08-23	✓
14	Критическая	CVE-2025-9179	Mozilla Thunderbird 140.x, Thunderbird ESR и Thunderbird	Сетевой	ACE	2025-08-23	✓
15	Высокая	CVE-2025-55231	Microsoft Windows storage-based management service	Сетевой	ACE	2025-08-22	✓
16	Высокая	CVE-2025-9132	Microsoft Edge	Сетевой	ACE	2025-08-22	✓

1

Краткое описание: Отказ в обслуживании в Cisco ASA and FTD

Идентификатор уязвимости: CVE-2025-20134
BDU:2025-10352

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: Cisco Adaptive Security Appliance (ASA):
9.12 - 9.15.1.21
Cisco Firepower Threat Defense (FTD):
6.0 - 6.7.0.4

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 4.6 AV:N/AC:L/AT:P/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: 2025-08-19 / 2025-08-19

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ssltls-dos-eHw76vZe
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwk44159
- https://bdu.fstec.ru/vul/2025-10352

2

Краткое описание: Подделка запросов на стороне сервера в Cisco Secure Firewall Management Center (FMC)

Идентификатор уязвимости: CVE-2025-20148
BDU:2025-10341

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

Уязвимый продукт: Cisco Secure Firewall Management Center (formerly Firepower Management Center, FMC): 7.0.6 - 7.4.2.1

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Подделка запросов на стороне сервера

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

Оценка CVSSv3: 8.5 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:N

Оценка CVSSv4: 1.3 AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:L/SI:L/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-15 / 2025-08-15

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-html-inj-MqjrZrny
- https://bdu.fstec.ru/vul/2025-10341

3

Краткое описание: Отказ в обслуживании в Cisco Secure Firewall Management Center (FMC) and Firepower Threat Defense (FTD)

Идентификатор уязвимости: CVE-2025-20217
BDU:2025-10353

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

Уязвимый продукт: Cisco Firepower Threat Defense (FTD):
7.1.0 - 7.6.0

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: 8.6 AV:N/AC:L/PR:N/UI:N/S:C/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: 2025-08-15 / 2025-08-15

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dos-SvKhtjgt
- https://bdu.fstec.ru/vul/2025-10353

Краткое описание: Отказ в обслуживании в Cisco ASA and FTD IPv6 over IPsec feature

Идентификатор уязвимости: CVE-2025-20222
BDU:2025-10342

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

Уязвимый продукт: Cisco Adaptive Security Appliance (ASA):
до 9.16.4.82, 9.19.1.42, 9.20.3.10, 9.20.4, 9.22.2, 9.23.1
Cisco Firepower Threat Defense (FTD):
до 7.0.7, 7.2.10, 7.4.2.3, 7.6.1, 7.7.0

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 4.6 AV:N/AC:L/AT:P/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: 2025-08-14 / 2025-08-14

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fp2k-IPsec-dos-tjwgdZCO
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwm95070
- https://bdu.fstec.ru/vul/2025-10342

5

Краткое описание: Выполнение произвольного кода в Google Chrome

Идентификатор уязвимости: CVE-2025-9478

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 139.0.7258.140

Категория уязвимого продукта: Не определено

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

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: Требуется

Дата выявления / Дата обновления: 2025-08-27 / 2025-08-27

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/08/stable-channel-update-for-desktop_26.html
- https://crbug.com/437825940

6

Краткое описание: Выполнение произвольного кода в Ansible Automation Platform 2.5 packages

Идентификатор уязвимости: CVE-2025-47273
BDU:2025-08604

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

Уязвимый продукт: python3.11-galaxy-ng (Red Hat package):
до 4.10.7-1.el8ap
python3.11-django-ansible-base (Red Hat package):
до 2.5.20250827-1.el8ap
python3.11-django (Red Hat package):
до 4.2.23-1.el8ap
automation-hub (Red Hat package):
до 4.10.7-1.el8ap
automation-gateway (Red Hat package):
до 2.5.20250827-1.el8ap
automation-eda-controller (Red Hat package):
до 1.1.13-1.el8ap
automation-controller (Red Hat package):
до 4.6.19-1.el8ap
ansible-automation-platform-installer (Red Hat package):
до 2.5-17.el8ap
Ansible Automation Platform:
до 2.5

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.8 AV:N/AC:L/PR:L/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: 2025-08-26 / 2025-08-26

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:14686
- https://bdu.fstec.ru/vul/2025-08604

7

Краткое описание: Отказ в обслуживании в Apache Kafka

Идентификатор уязвимости: CVE-2025-27819
BDU:2025-08199

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: Apache Kafka:
2.0.0 - 3.3.2

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 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:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-26 / 2025-08-26

Ссылки на источник:

- https://kafka.apache.org/cve-list
- https://bdu.fstec.ru/vul/2025-08199

8

Краткое описание: Выполнение произвольного кода в Rockwell Automation Arena

Идентификатор уязвимости: CVE-2025-6377

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Arena:
- - 16.20.08

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

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: 2025-08-25 / 2025-08-25

Ссылки на источник:

- https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1729.html
- https://www.zerodayinitiative.com/advisories/ZDI-25-837/

Краткое описание: Выполнение произвольного кода в Rockwell Automation Arena

Идентификатор уязвимости: CVE-2025-6376
BDU:2025-08441

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Arena:
- - 16.20.08

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

9 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2025-08-25 / 2025-08-25

Ссылки на источник:

- https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1729.html
- https://www.zerodayinitiative.com/advisories/ZDI-25-836/
- https://bdu.fstec.ru/vul/2025-08441

10

Краткое описание: Обход безопасности в Mozilla Thunderbird 140.x, Thunderbird ESR и Thunderbird

Идентификатор уязвимости: CVE-2025-9185
BDU:2025-10497

Идентификатор программной ошибки: CWE-254 Уязвимости в безопасности ПО

Уязвимый продукт: Mozilla Thunderbird:
140.0 - 140.1
Mozilla Thunderbird:
130.0 - 141.0
Mozilla Thunderbird:
102.0 - 128.13

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Обход безопасности

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

Оценка CVSSv3: 8.1 AV:N/AC:H/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:L/VA:N/SC:L/SI:L/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-23 / 2025-08-23

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-72/
- https://bdu.fstec.ru/vul/2025-10497
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-71/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-70/

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird 140.x и Thunderbird

Идентификатор уязвимости: CVE-2025-9184
BDU:2025-10502

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

Уязвимый продукт: Mozilla Thunderbird:
140.0 - 140.1
Mozilla Thunderbird:
130.0 - 141.0

Категория уязвимого продукта: Не определено

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

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2025-08-23 / 2025-08-23

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-72/
- https://bdu.fstec.ru/vul/2025-10502
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-70/

Краткое описание: Отказ в обслуживании в Mozilla Thunderbird 140.x и Thunderbird

Идентификатор уязвимости: CVE-2025-9182
BDU:2025-10388

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

Уязвимый продукт: Mozilla Thunderbird:
140.0 - 140.1
Mozilla Thunderbird:
130.0 - 141.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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: 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/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: 2025-08-23 / 2025-08-23

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-72/
- https://bdu.fstec.ru/vul/2025-10388
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-70/

13

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird 140.x, Thunderbird ESR и Thunderbird

Идентификатор уязвимости: CVE-2025-9180
BDU:2025-10385

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

Уязвимый продукт: Mozilla Thunderbird:
140.0 - 140.1
Mozilla Thunderbird:
130.0 - 141.0
Mozilla Thunderbird:
102.0 - 128.13

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.1 AV:N/AC:L/PR:N/UI:R/S:U/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: 2025-08-23 / 2025-08-23

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-72/
- https://bdu.fstec.ru/vul/2025-10385
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-71/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-70/

14

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird 140.x, Thunderbird ESR и Thunderbird

Идентификатор уязвимости: CVE-2025-9179
BDU:2025-10496

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

Уязвимый продукт: Mozilla Thunderbird:
140.0 - 140.1
Mozilla Thunderbird:
130.0 - 141.0
Mozilla Thunderbird:
102.0 - 128.13

Категория уязвимого продукта: Не определено

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2025-08-23 / 2025-08-23

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-72/
- https://bdu.fstec.ru/vul/2025-10496
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-71/
- https://www.mozilla.org/en-US/security/advisories/mfsa2025-70/

Краткое описание: Выполнение произвольного кода в Microsoft Windows storage-based management service

Идентификатор уязвимости: CVE-2025-55231

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

Уязвимый продукт: Windows Server:
2012 Gold - 2025 10.0.26100.4946
Microsoft IIS:
10.0 - 10.0.08608

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

15

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 2025-08-22 / 2025-08-22

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-55231

16

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2025-9132

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Microsoft Edge:
100.0.1185.29 - 139.0.3405.102

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

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: 2025-08-22 / 2025-08-22

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-9132