НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-10-09.1 | 9 октября 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2025-59681	Django	Сетевой	ACE	2025-10-03	✓
2	Высокая	CVE-2025-40738	Siemens SINEC NMS	Сетевой	ACE	2025-10-02	✓
3	Высокая	CVE-2025-40737	Siemens SINEC NMS	Сетевой	ACE	2025-10-02	✓
4	Критическая	CVE-2025-40736	Siemens SINEC NMS	Сетевой	OSI	2025-10-02	✓
5	Высокая	CVE-2025-40735	Siemens SINEC NMS	Сетевой	ACE	2025-10-02	✓
6	Высокая	CVE-2025-40764	Siemens Simcenter Femap	Локальный	ACE	2025-10-02	✓
7	Высокая	CVE-2025-40762	Siemens Simcenter Femap	Локальный	ACE	2025-10-02	✓
8	Высокая	CVE-2025-40758	Siemens Mendix SAML Module	Сетевой	OSI	2025-10-02	✓
9	Высокая	CVE-2025-11153	Mozilla Firefox	Сетевой	ACE	2025-10-01	✓
10	Высокая	CVE-2025-11152	Mozilla Firefox	Сетевой	ACE	2025-10-01	✓
11	Высокая	CVE-2025-9900	Libtiff	Сетевой	ACE	2025-09-30	✓
12	Высокая	CVE-2025-41244	VMware products	Локальный	PE	2025-09-30	✓
13	Высокая	CVE-2025-57637	D-Link DI-7100G	Сетевой	ACE	2025-09-30	✗

14	Высокая	CVE-2025-57833	Ansible Automation Platform 2.5 packages	Сетевой	ACE	2025-09-29	✓
15	Высокая	CVE-2025-47273	Multicluster Engine for Kubernetes 2.8	Сетевой	OAF	2025-09-29	✓
16	Критическая	CVE-2025-22871	Multicluster Engine for Kubernetes 2.8	Сетевой	ACE	2025-09-29	✓
17	Высокая	CVE-2025-8941	Multicluster Engine for Kubernetes 2.8	Локальный	PE	2025-09-29	✓
18	Высокая	CVE-2025-8194	Multicluster Engine for Kubernetes 2.8	Сетевой	DoS	2025-09-29	✓
19	Критическая	CVE-2025-6965	Multicluster Engine for Kubernetes 2.8	Сетевой	DoS	2025-09-29	✓
20	Высокая	CVE-2025-6020	Multicluster Engine for Kubernetes 2.8	Локальный	ACE	2025-09-29	✓
21	Критическая	CVE-2024-52533	Multicluster Engine for Kubernetes 2.8	Сетевой	ACE	2025-09-29	✓
22	Высокая	CVE-2025-30204	Multicluster Engine for Kubernetes 2.8	Сетевой	DoS	2025-09-29	✓

1

Краткое описание: Выполнение произвольного кода в Django

Идентификатор уязвимости: CVE-2025-59681
BDU:2025-12461

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

Уязвимый продукт: Django:
4.2 - 5.2.6

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.1 AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-10-03 / 2025-10-03

Ссылки на источник:

- https://www.djangoproject.com/weblog/2025/oct/01/security-releases/
- https://bdu.fstec.ru/vul/2025-12461

2

Краткое описание: Выполнение произвольного кода в Siemens SINEC NMS

Идентификатор уязвимости: CVE-2025-40738
BDU:2025-08985

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

Уязвимый продукт: SINEC NMS:
до 4.0

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2025-10-02 / 2025-10-02

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-078892.html
- https://bdu.fstec.ru/vul/2025-08985

3

Краткое описание: Выполнение произвольного кода в Siemens SINEC NMS

Идентификатор уязвимости: CVE-2025-40737
BDU:2025-08984

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

Уязвимый продукт: SINEC NMS:
до 4.0

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2025-10-02 / 2025-10-02

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-078892.html
- https://bdu.fstec.ru/vul/2025-08984

4

Краткое описание: Получение конфиденциальной информации в Siemens SINEC NMS

Идентификатор уязвимости: CVE-2025-40736
BDU:2025-08268

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

Уязвимый продукт: SINEC NMS:
до 4.0

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Обход процесса аутентификации

Последствия эксплуатации: Получение конфиденциальной информации

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

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

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: 2025-10-02 / 2025-10-02

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-078892.html
- https://bdu.fstec.ru/vul/2025-08268

Краткое описание: Выполнение произвольного кода в Siemens SINEC NMS

Идентификатор уязвимости: CVE-2025-40735
BDU:2025-08986

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

Уязвимый продукт: SINEC NMS:
до 4.0

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

5 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2025-10-02 / 2025-10-02

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-078892.html
- https://bdu.fstec.ru/vul/2025-08986

6

Краткое описание: Выполнение произвольного кода в Siemens Simcenter Femap

Идентификатор уязвимости: CVE-2025-40764
BDU:2025-10822

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: Simcenter Femap:
2406 - 2412

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: 2025-10-02 / 2025-10-02

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-674084.html
- https://bdu.fstec.ru/vul/2025-10822

7

Краткое описание: Выполнение произвольного кода в Siemens Simcenter Femap

Идентификатор уязвимости: CVE-2025-40762
BDU:2025-10821

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Simcenter Femap:
2406 - 2412

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: 2025-10-02 / 2025-10-02

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-674084.html
- https://bdu.fstec.ru/vul/2025-10821

8

Краткое описание: Получение конфиденциальной информации в Siemens Mendix SAML Module

Идентификатор уязвимости: CVE-2025-40758

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: Mendix SAML Module:
до 3.6.21

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

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

Оценка CVSSv4: 6.9 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/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: 2025-10-02 / 2025-10-02

Ссылки на источник:

- https://cert-portal.siemens.com/productcert/html/ssa-395458.html

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-11153

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

Уязвимый продукт: Mozilla Firefox:
140.0 - 143.0.1
Firefox for Android:
140.0 - 143.0

Категория уязвимого продукта: Не определено

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

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

Дата выявления / Дата обновления: 2025-10-01 / 2025-10-01

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-80/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1987481

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-11152

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

Уязвимый продукт: Mozilla Firefox:
140.0 - 143.0.1
Firefox for Android:
140.0 - 143.0

Категория уязвимого продукта: Не определено

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

Последствия эксплуатации: Выполнение произвольного кода

10 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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:U/C:L/I:H/A:L

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: 2025-10-01 / 2025-10-01

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-80/
- https://bugzilla.mozilla.org/show_bug.cgi?id=1987246

Краткое описание: Выполнение произвольного кода в Libtiff

Идентификатор уязвимости: CVE-2025-9900

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

Уязвимый продукт: LibTIFF:
4.0 - 4.7.0

Категория уязвимого продукта: Не определено

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

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: 8.8 AV:N/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: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-30 / 2025-09-30

Ссылки на источник:

- https://bugzilla.redhat.com/show_bug.cgi?id=2392784
- https://github.com/SexyShoelessGodofWar/LibTiff-4.7.0-Write-What-Where?tab=readme-ov-file

Краткое описание: Повышение привилегий в VMware products

Идентификатор уязвимости: CVE-2025-41244
BDU:2025-12421

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: VMware Tools: 11.0.0 - 13.0.1.0
VMware Aria Operations (formerly vRealize Operations): 8.0.0 - 8.18.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

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.

12

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: 2025-09-30 / 2025-09-30

Ссылки на источник:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/36149
- https://blog.nviso.eu/2025/09/29/you-name-it-vmware-elevates-it-cve-2025-41244/
- https://bdu.fstec.ru/vul/2025-12421

13

Краткое описание: Выполнение произвольного кода в D-Link DI-7100G

Идентификатор уязвимости: CVE-2025-57637

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

Уязвимый продукт: DI-7100G:
все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 8.9 AV:N/AC:L/AT:N/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: 2025-09-30 / 2025-09-30

Ссылки на источник:

- https://supportannouncement.us.dlink.com/security/publication.aspx?name=SAP10470
- https://github.com/glkfc/IoT-Vulnerability/blob/main/D-Link/Dlink_2.md

14	**Краткое описание:** Выполнение произвольного кода в Ansible Automation Platform 2.5 packages **Идентификатор уязвимости:** CVE-2025-57833 BDU:2025-11748 **Идентификатор программной ошибки:** CWE-89 Некорректная нейтрализация специальных элементов, используемых в SQL-командах (внедрение SQL-кода) **Уязвимый продукт:** python3.11-tox-ansible (Red Hat package): до 25.8.0-1.el8ap python3.11-termcolor (Red Hat package): до 3.1.0-1.el8ap python3.11-ruamel-yaml (Red Hat package): до 0.18.15-1.el8ap python3.11-pytest-sugar (Red Hat package): до 1.1.1-1.el8ap python3.11-pytest-plus (Red Hat package): до 0.8.1-1.el8ap python3.11-pytest-ansible (Red Hat package): до 25.8.0-1.el8ap python3.11-galaxy-ng (Red Hat package): до 4.10.8-1.el8ap python3.11-galaxy-importer (Red Hat package): до 0.4.33-1.el8ap python3.11-django-ansible-base (Red Hat package): до 2.5.20250924-1.el8ap python3.11-django (Red Hat package): до 4.2.24-1.el8ap python3.11-ansible-compat (Red Hat package): до 25.8.1-1.el8ap molecule (Red Hat package): до 25.7.0-1.el8ap automation-hub (Red Hat package): до 4.10.8-1.el8ap automation-gateway-proxy (Red Hat package): до 2.6.6-3.el9ap

automation-gateway (Red Hat package):
до 2.5.20250924-2.el8ap
automation-controller (Red Hat package):
до 4.6.20-1.el8ap
ansible-sign (Red Hat package):
до 0.1.2-1.el8ap
ansible-navigator (Red Hat package):
до 25.8.0-1.el8ap
ansible-lint (Red Hat package):
до 25.8.2-1.el8ap
ansible-dev-tools (Red Hat package):
до 25.8.3-1.el8ap
ansible-dev-environment (Red Hat package):
до 25.8.0-1.el8ap
ansible-creator (Red Hat package):
до 25.8.0-1.el8ap
ansible-automation-platform-installer (Red Hat package):
до 2.5-18.el8ap
aap-metrics-utility (Red Hat package):
до 0.6.0-2.el8ap
Ansible Automation Platform:
до 2.5

Категория уязвимого продукта: Универсальные компоненты и библиотеки

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.1 AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-29 / 2025-09-29

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:16487
- https://bdu.fstec.ru/vul/2025-11748

Краткое описание: Перезапись произвольных файлов в Multicluster Engine for Kubernetes 2.8

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

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

Уязвимый продукт: Multicluster Engine for Kubernetes:
до 2.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Перезапись произвольных файлов

15 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: 2025-09-29 / 2025-09-29

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:16101
- https://bdu.fstec.ru/vul/2025-08604

16

Краткое описание: Выполнение произвольного кода в Multicluster Engine for Kubernetes 2.8

Идентификатор уязвимости: CVE-2025-22871
BDU:2025-04014

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

Уязвимый продукт: Multicluster Engine for Kubernetes:
до 2.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 2.7 AV:N/AC:L/AT:N/PR:N/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: 2025-09-29 / 2025-09-29

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:16101
- https://bdu.fstec.ru/vul/2025-04014

17

Краткое описание: Повышение привилегий в Multicluster Engine for Kubernetes 2.8

Идентификатор уязвимости: CVE-2025-8941

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

Уязвимый продукт: Multicluster Engine for Kubernetes:
до 2.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Повышение привилегий

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

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-29 / 2025-09-29

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:16101

18

Краткое описание: Отказ в обслуживании в Multicluster Engine for Kubernetes 2.8

Идентификатор уязвимости: CVE-2025-8194
BDU:2025-09687

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

Уязвимый продукт: Multicluster Engine for Kubernetes:
до 2.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

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: 1.2 AV:L/AC:L/AT:N/PR:N/UI:N/VC:N/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: 2025-09-29 / 2025-09-29

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:16101
- https://bdu.fstec.ru/vul/2025-09687

19

Краткое описание: Отказ в обслуживании в Multicluster Engine for Kubernetes 2.8

Идентификатор уязвимости: CVE-2025-6965
BDU:2025-08786

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

Уязвимый продукт: Multicluster Engine for Kubernetes:
до 2.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

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

Оценка CVSSv4: 2.7 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/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: 2025-09-29 / 2025-09-29

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:16101
- https://bdu.fstec.ru/vul/2025-08786

Краткое описание: Выполнение произвольного кода в Multicluster Engine for Kubernetes 2.8

Идентификатор уязвимости: CVE-2025-6020
BDU:2025-07273

Идентификатор программной ошибки: CWE-284 Некорректное управление доступом

Уязвимый продукт: Multicluster Engine for Kubernetes:
до 2.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование ситуации гонки (race condition) в системе.

Последствия эксплуатации: Выполнение произвольного кода

20

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: 5.9 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-29 / 2025-09-29

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:16101
- https://bdu.fstec.ru/vul/2025-07273

21

Краткое описание: Выполнение произвольного кода в Multicluster Engine for Kubernetes 2.8

Идентификатор уязвимости: CVE-2024-52533
BDU:2024-10796

Идентификатор программной ошибки: CWE-193 Ошибка смещения на единицу

Уязвимый продукт: Multicluster Engine for Kubernetes:
до 2.8.3

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подключение к вредоносному серверу.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2025-09-29 / 2025-09-29

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:16101
- https://bdu.fstec.ru/vul/2024-10796

22

Краткое описание: Отказ в обслуживании в Multicluster Engine for Kubernetes 2.8

Идентификатор уязвимости: CVE-2025-30204
BDU:2025-08472

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

Уязвимый продукт: Multicluster Engine for Kubernetes:
до 2.8.3

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.

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: 2025-09-29 / 2025-09-29

Ссылки на источник:

- https://access.redhat.com/errata/RHSA-2025:16101
- https://bdu.fstec.ru/vul/2025-08472