НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-08-21.1 | 21 августа 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2025-44643	VigorAP 903, VigorAP 912C, VigorAP 918R	Сетевой	LoI	2025-08-04	✗
2	Высокая	CVE-2025-49561	Adobe Animate 2023, Adobe Animate 2024	Локальный	ACE	2025-08-12	✓
3	Высокая	CVE-2025-49573	Adobe Substance 3D Modeler	Локальный	ACE	2025-08-12	✓
4	Высокая	CVE-2025-49572	Adobe Substance 3D Modeler	Локальный	ACE	2025-08-12	✓
5	Высокая	CVE-2025-49571	Adobe Substance 3D Modeler	Локальный	ACE	2025-08-12	✓
6	Высокая	CVE-2025-49570	Photoshop 2025, Photoshop 2024	Локальный	ACE	2025-08-12	✓
7	Высокая	CVE-2025-49564	Illustrator 2025, Illustrator 2024	Локальный	ACE	2025-08-12	✓
8	Высокая	CVE-2025-49563	Illustrator 2025, Illustrator 2024	Локальный	ACE	2025-08-12	✓
9	Высокая	CVE-2025-52970	FortiWeb	Сетевой	LoI	2025-08-12	✓
10	Высокая	CVE-2025-50154	Windows	Сетевой	LoI	2025-08-12	✓
11	Высокая	CVE-2025-8715	Postgres Pro Certified, PostgreSQL	Сетевой	ACE	2025-08-13	✓
12	Высокая	CVE-2025-8714	Postgres Pro Certified, PostgreSQL	Сетевой	ACE	2025-08-13	✓
13	Критическая	CVE-2025-20265	Cisco Secure Firewall Management Center	Сетевой	ACE	2025-08-14	✓

14	Критическая	CVE-2025-40746	SIMATIC RTLS Locating Manager	Сетевой	ACE	2025-08-12	✓
15	Критическая	CVE-2025-25256	FortiSIEM	Сетевой	PE	2025-08-12	✓
16	Высокая	CVE-2025-53737	Microsoft Excel, Microsoft Office, 365 Apps for Enterprise, Microsoft Office for Mac	Локальный	ACE	2025-08-12	✓
17	Высокая	CVE-2025-53735	Microsoft Excel, Microsoft Office, 365 Apps for Enterprise, Microsoft Office for Mac	Локальный	ACE	2025-08-12	✓
18	Высокая	CVE-2025-49560	Adobe Substance 3D Modeler	Локальный	ACE	2025-08-12	✓
19	Высокая	CVE-2025-49569	Adobe Substance 3D Modeler	Локальный	ACE	2025-08-12	✓
20	Высокая	CVE-2025-53733	Microsoft SharePoint Enterprise Server, Microsoft Word, Microsoft Office, Microsoft SharePoint Server, 365 Apps for Enterprise, Microsoft Office for Mac	Локальный	ACE	2025-08-12	✓
21	Критическая	CVE-2025-53766	Windows	Сетевой	ACE	2025-08-12	✓
22	Высокая	CVE-2025-53784	365 Apps for Enterprise, Microsoft Office, Microsoft Office for Mac	Локальный	ACE	2025-08-12	✓
23	Высокая	CVE-2025-53778	Windows	Сетевой	PE	2025-08-12	✓
24	Высокая	CVE-2025-23320	NVIDIA Triton Inference Server	Сетевой	Lol	2025-08-04	✓
25	Критическая	CVE-2025-23310	NVIDIA Triton Inference Server	Сетевой	DoS	2025-08-04	✓

26	Высокая	CVE-2025-23331	NVIDIA Triton Inference Server	Сетевой	DoS	2025-08-04	✓
27	Высокая	CVE-2025-8810	Tenda AC20	Сетевой	DoS	2025-08-02	✗
28	Высокая	CVE-2025-8816	Linksys RE6500, RE6250, RE6300, RE6350, RE7000, RE9000	Сетевой	ACE	2025-08-01	✗
29	Высокая	CVE-2025-8817	Linksys RE6500, RE6250, RE6300, RE6350, RE7000, RE9000	Сетевой	ACE	2025-08-01	✗
30	Высокая	CVE-2025-8819	Linksys RE6500, RE6250, RE6300, RE6350, RE7000, RE9000	Сетевой	ACE	2025-08-01	✗
31	Высокая	CVE-2025-3320	IBM Tivoli Monitoring	Сетевой	ACE	2025-08-05	✓
32	Высокая	CVE-2025-3354	IBM Tivoli Monitoring	Сетевой	DoS	2025-08-05	✓
33	Высокая	CVE-2025-8832	Linksys RE6250, Linksys RE6500, Linksys RE6300, Linksys RE6350, Linksys RE7000, Linksys RE9000	Сетевой	ACE	2025-08-01	✗
34	Высокая	CVE-2025-7771	ThrottleStop	Локальный	ACE	2025-08-06	✗
35	Высокая	CVE-2025-54923	EcoStruxure Power Monitoring Expert, EcoStruxure PowerOperation (EPO) - Advanced Reporting and Dashboards Module	Сетевой	LoI	2025-08-12	✓
36	Высокая	CVE-2025-8831	Linksys RE6250, Linksys RE6500, Linksys RE6300, Linksys RE6350, Linksys RE7000, Linksys RE9000	Сетевой	ACE	2025-08-01	✗

37	Высокая	CVE-2025-8820	Linksys RE6250, Linksys RE6500, Linksys RE6300, Linksys RE6350, Linksys RE7000, Linksys RE9000	Сетевой	DoS	2025-08-01	✗
38	Высокая	CVE-2025-8824	Linksys RE6250, Linksys RE6500, Linksys RE6300, Linksys RE6350, Linksys RE7000, Linksys RE9000	Сетевой	DoS	2025-08-01	✗
39	Высокая	CVE-2025-8822	Linksys RE6250, Linksys RE6500, Linksys RE6300, Linksys RE6350, Linksys RE7000, Linksys RE9000	Сетевой	DoS	2025-08-01	✗
40	Высокая	CVE-2025-23322	NVIDIA Triton Inference Server	Сетевой	DoS	2025-08-04	✓
41	Критическая	CVE-2025-23318	NVIDIA Triton Inference Server	Сетевой	DoS	2025-08-04	✗
42	Критическая	CVE-2025-23311	NVIDIA Triton Inference Server	Сетевой	DoS	2025-08-04	✓
43	Высокая	CVE-2025-23324	NVIDIA Triton Inference Server	Сетевой	DoS	2025-08-04	✓
44	Высокая	CVE-2025-23321	NVIDIA Triton Inference Server	Сетевой	DoS	2025-08-04	✓
45	Высокая	CVE-2025-23327	NVIDIA Triton Inference Server	Сетевой	DoS	2025-08-04	✓
46	Высокая	CVE-2025-23325	NVIDIA Triton Inference Server	Сетевой	DoS	2025-08-04	✓
47	Критическая	CVE-2025-23317	NVIDIA Triton Inference Server	Сетевой	ACE	2025-08-04	✓
48	Высокая	CVE-2025-23326	NVIDIA Triton Inference Server	Сетевой	DoS	2025-08-04	✓
49	Высокая	CVE-2025-23323	NVIDIA Triton Inference Server	Сетевой	DoS	2025-08-04	✓

50	Критическая	CVE-2025-53767	Azure Open AI	Сетевой	PE	2025-08-07	✓
51	Критическая	CVE-2025-54987	Apex One	Сетевой	ACE	2025-08-01	✓
52	Высокая	CVE-2025-8826	Linksys RE6250, Linksys RE6500, Linksys RE6300, Linksys RE6350, Linksys RE7000, Linksys RE9000	Сетевой	ACE	2025-08-01	✗
53	Критическая	CVE-2025-5999	Vault Enterprise, Vault Community Edition	Сетевой	PE	2025-08-01	✓
54	Высокая	CVE-2025-38747	Dell SupportAssist OS Recovery	Локальный	PE	2025-08-06	✓
55	Высокая	CVE-2025-54627	HarmonyOS	Сетевой	LoI	2025-08-05	✓
56	Критическая	CVE-2025-22470	SATO CL4NX Plus, SATO CL4NX-J Plus, SATO CL6NX Plus, SATO CL6NX-J Plus	Сетевой	ACE	2025-08-04	✓
57	Критическая	CVE-2025-7768	Cloud Connect Advanced (CCA)	Сетевой	PE	2025-08-05	✗
58	Высокая	CVE-2025-7769	Cloud Connect Advanced (CCA)	Сетевой	PE	2025-08-05	✗
59	Высокая	CVE-2025-7770	Cloud Connect Advanced (CCA)	Сетевой	LoI	2025-08-05	✗
60	Критическая	CVE-2025-54987	Apex One	Сетевой	ACE	2025-08-01	✓
61	Высокая	CVE-2025-5999	Vault Enterprise, Vault Community Edition	Сетевой	PE	2025-08-01	✓
62	Критическая	CVE-2025-6000	Vault Enterprise, Vault Community Edition	Сетевой	ACE	2025-08-01	✓

63	Критическая	CVE-2025-54887	JSON Web Encryption (JWE)	Сетевой	LoI	2025-08-07	✓
64	Высокая	CVE-2025-54254	Adobe Experience Manager (AEM) Forms on JEE	Сетевой	RLF	2025-08-05	✓
65	Высокая	CVE-2025-54634	HarmonyOS	Локальный	LoI	2025-08-05	✓
66	Высокая	CVE-2025-7025	Arena Simulation	Локальный	ACE	2025-08-05	✓
67	Высокая	CVE-2025-23319	NVIDIA Triton Inference Server	Сетевой	ACE	2025-08-04	✓
68	Критическая	CVE-2025-54253	Adobe Experience Manager (AEM) Forms on JEE	Сетевой	ACE	2025-08-05	✓
69	Критическая	CVE-2025-48530	Android	Сетевой	ACE	2025-08-01	✓
70	Высокая	CVE-2025-22441	Android	Локальный	PE	2025-08-01	✓
71	Высокая	CVE-2025-48533	Android	Локальный	PE	2025-08-01	✓
72	Высокая	CVE-2025-23276	NVIDIA Corp.	Локальный	ACE	2025-08-02	✓
73	Критическая	CVE-2025-54574	Squid Software Foundation	Сетевой	ACE	2025-08-01	✓
74	Высокая	CVE-2024-26009	Fortinet products	Сетевой	ACE	2025-08-12	✓
75	Критическая	CVE-2025-7353	Rockwell Automation	Сетевой	ACE	2025-08-14	✓
76	Высокая	BDU:2025-09997	Elastic NV	Локальный	DoS	2025-08-18	✗

1

Краткое описание: Потеря целостности в VigorAP 903, VigorAP 912C, VigorAP 918R

Идентификатор уязвимости: CVE-2025-44643
BDU:2025-09910

Идентификатор программной ошибки: CWE-276 Некорректные разрешения, назначаемые по умолчанию

Уязвимый продукт: 1.4.18 (VigorAP 903), 1.4.9 (VigorAP 912C), 1.4.9 (VigorAP 918R)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Использование жестко закодированных учетных данных

Последствия эксплуатации: Потеря целостности

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09910
- https://www.notion.so/Misconfiguration-in-Draytek-AP903-23a54a1113e780aca7f2d21dbdab9db8
- https://vuldb.com/?id.318689"

2

Краткое описание: Выполнение произвольного кода в Adobe Animate 2023, Adobe Animate 2024

Идентификатор уязвимости: CVE-2025-49561
BDU:2025-09896

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: до 23.0.12 включительно (Adobe Animate 2023), до 24.0.9 включительно (Adobe Animate 2024)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09896
- https://helpx.adobe.com/security/products/animate/apsb25-73.html

3

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

Идентификатор уязвимости: CVE-2025-49573
BDU:2025-09895

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: до 1.22.2 (Adobe Substance 3D Modeler)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Запись за пределами буфера.

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: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09895
- https://helpx.adobe.com/security/products/substance3d-modeler/apsb25-76.html

4

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

Идентификатор уязвимости: CVE-2025-49572
BDU:2025-09894

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: до 1.22.2 (Adobe Substance 3D Modeler)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Запись за пределами буфера.

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: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09894
- https://helpx.adobe.com/security/products/substance3d-modeler/apsb25-76.html

5

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

Идентификатор уязвимости: CVE-2025-49571
BDU:2025-09893

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: до 1.22.2 (Adobe Substance 3D Modeler)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09893

6

Краткое описание: Выполнение произвольного кода в Photoshop 2025, Photoshop 2024

Идентификатор уязвимости: CVE-2025-49570
BDU:2025-09890

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: до 26.9 (Photoshop 2025), до 25.12.4 (Photoshop 2024)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Запись за пределами буфера.

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: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09890

Краткое описание: Выполнение произвольного кода в Illustrator 2025, Illustrator 2024

Идентификатор уязвимости: CVE-2025-49564
BDU:2025-09889

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: до 29.7 (Illustrator 2025), до 28.7.9 (Illustrator 2024)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

7 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09889
- https://helpx.adobe.com/security/products/illustrator/apsb25-74.html

8

Краткое описание: Выполнение произвольного кода в Illustrator 2025, Illustrator 2024

Идентификатор уязвимости: CVE-2025-49563
BDU:2025-09888

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: до 29.7 (Illustrator 2025), до 28.7.9 (Illustrator 2024)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Запись за пределами буфера.

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: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09888
- https://helpx.adobe.com/security/products/illustrator/apsb25-74.html

9

Краткое описание: Потеря целостности в FortiWeb

Идентификатор уязвимости: CVE-2025-52970
BDU:2025-09849

Идентификатор программной ошибки: CWE-233 Некорректная обработка параметров

Уязвимый продукт: от 7.2.0 до 7.2.11 (FortiWeb), от 7.6.0 до 7.6.4 (FortiWeb), от 7.4.0 до 7.4.8 (FortiWeb)

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Потеря целостности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09849
- https://fortiguard.fortinet.com/psirt/FG-IR-25-448
- https://pwner.gg/blog/2025-08-13-fortiweb-cve-2025-52970"

10

Краткое описание: Потеря целостности в Windows

Идентификатор уязвимости: CVE-2025-50154
BDU:2025-09832

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

Уязвимый продукт: Server 2008 R2 SP1 (Windows), Server 2008 SP2 (Windows), Server 2008 SP2 (Windows), Server 2012 (Windows), Server 2012 R2 (Windows), 10 (Windows), 10 (Windows), 10 1607 (Windows), 10 1607 (Windows), Server 2016 (Windows), Server 2008 SP2 Server Core installation (Windows), Server 2008 SP2 Server Core installation (Windows), Server 2012 R2 Server Core installation (Windows), Server 2016 Server Core installation (Windows), Server 2008 R2 SP1 Server Core installation (Windows), Server 2012 Server Core installation (Windows), 10 1809 (Windows), 10 1809 (Windows), Server 2019 (Windows), Server 2019 Server Core installation (Windows), Server 2022 (Windows), Server 2022 Server Core installation (Windows), 10 21H2 (Windows), 10 21H2 (Windows), 10 21H2 (Windows), 11 22H2 (Windows), 11 22H2 (Windows), 10 22H2 (Windows), 10 22H2 (Windows), 10 22H2 (Windows), 11 23H2 (Windows), 11 23H2 (Windows), Server 2022 23H2 Edition Server Core installation (Windows), 11 24H2 (Windows), 11 24H2 (Windows), Server 2025 (Windows), Server 2025 Server Core installation (Windows)

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Потеря целостности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09832
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-50154

- https://cymulate.com/blog/zero-click-one-ntlm-microsoft-security-patch-bypass-cve-2025-50154/"

Краткое описание: Выполнение произвольного кода в Postgres Pro Certified, PostgreSQL

Идентификатор уязвимости: CVE-2025-8715
BDU:2025-09830

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

Уязвимый продукт: до 17.5 (Postgres Pro Certified), до 16.9 (Postgres Pro Certified), до 15.13 (Postgres Pro Certified), до 14.18 (Postgres Pro Certified), до 13.21 (Postgres Pro Certified), от 17.0 до 17.6 (PostgreSQL), от 16.0 до 16.10 (PostgreSQL), от 15.0 до 15.14 (PostgreSQL), от 14.0 до 14.19 (PostgreSQL), от 13.0 до 13.22 (PostgreSQL)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Инъекция.

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: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-13 / 2025-08-13

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09830
- https://www.postgresql.org/support/security/CVE-2025-8715/
- https://postgrespro.ru/products/postgrespro/certified"

Краткое описание: Выполнение произвольного кода в Postgres Pro Certified, PostgreSQL

Идентификатор уязвимости: CVE-2025-8714
BDU:2025-09829

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

Уязвимый продукт: до 17.5 (Postgres Pro Certified), до 16.9 (Postgres Pro Certified), до 15.13 (Postgres Pro Certified), до 14.18 (Postgres Pro Certified), до 13.21 (Postgres Pro Certified), от 17.0 до 17.6 (PostgreSQL), от 16.0 до 16.10 (PostgreSQL), от 15.0 до 15.14 (PostgreSQL), от 14.0 до 14.19 (PostgreSQL), от 13.0 до 13.22 (PostgreSQL)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Инъекция.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-13 / 2025-08-13

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09829
- https://www.postgresql.org/support/security/CVE-2025-8714/
- https://postgrespro.ru/products/postgrespro/certified"

13

Краткое описание: Выполнение произвольного кода в Cisco Secure Firewall Management Center

Идентификатор уязвимости: CVE-2025-20265
BDU:2025-09828

Идентификатор программной ошибки: CWE-74 Некорректная нейтрализация специальных элементов в выходных данных, отправляемых клиенту (внедрение)

Уязвимый продукт: 7.0.7 (Cisco Secure Firewall Management Center), 7.7.0 (Cisco Secure Firewall Management Center)

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-14 / 2025-08-14

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09828
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-radius-rce-TNBKf79

14

Краткое описание: Выполнение произвольного кода в SIMATIC RTLS Locating Manager

Идентификатор уязвимости: CVE-2025-40746
BDU:2025-09822

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: до 3.2 (SIMATIC RTLS Locating Manager)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Некорректная проверка входных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09822
- https://cert-portal.siemens.com/productcert/html/ssa-493787.html

Краткое описание: Повышение привилегий в FortiSIEM

Идентификатор уязвимости: CVE-2025-25256
BDU:2025-09821

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

Уязвимый продукт: от 7.3 до 7.3.2 (FortiSIEM), от 7.2 до 7.2.6 (FortiSIEM), от 7.1 до 7.1.8 (FortiSIEM), от 7.0 до 7.0.4 (FortiSIEM), от 6.7 до 6.7.10 (FortiSIEM), от 5.4 до 6.6.5 включительно (FortiSIEM)

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09821
- https://fortiguard.fortinet.com/psirt/FG-IR-25-152
- https://www.theregister.com/2025/08/13/fortinet_discloses_critical_bug/"

16

Краткое описание: Выполнение произвольного кода в Microsoft Excel, Microsoft Office, 365 Apps for Enterprise, Microsoft Office for Mac

Идентификатор уязвимости: CVE-2025-53737
BDU:2025-09810

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

Уязвимый продукт: 2016 (Microsoft Excel), 2016 (Microsoft Excel), 2019 (Microsoft Office), 2019 (Microsoft Office), - (365 Apps for Enterprise), - (365 Apps for Enterprise), Online Server (Microsoft Office), LTSC 2021 (Microsoft Office), LTSC 2021 (Microsoft Office), LTSC 2021 (Microsoft Office for Mac), LTSC 2024 (Microsoft Office), LTSC 2024 (Microsoft Office), LTSC 2024 (Microsoft Office for Mac)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

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: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09810
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53737

17

Краткое описание: Выполнение произвольного кода в Microsoft Excel, Microsoft Office, 365 Apps for Enterprise, Microsoft Office for Mac

Идентификатор уязвимости: CVE-2025-53735
BDU:2025-09808

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: 2016 (Microsoft Excel), 2016 (Microsoft Excel), 2019 (Microsoft Office), 2019 (Microsoft Office), - (365 Apps for Enterprise), - (365 Apps for Enterprise), Online Server (Microsoft Office), LTSC 2021 (Microsoft Office), LTSC 2021 (Microsoft Office), LTSC 2021 (Microsoft Office for Mac), LTSC 2024 (Microsoft Office), LTSC 2024 (Microsoft Office), LTSC 2024 (Microsoft Office for Mac)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09808
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53735

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

Идентификатор уязвимости: CVE-2025-49560
BDU:2025-09806

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

Уязвимый продукт: до 1.22.2 (Adobe Substance 3D Modeler)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

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.

18

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09806
- https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-72.html

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

Идентификатор уязвимости: CVE-2025-49569
BDU:2025-09805

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: до 1.22.2 (Adobe Substance 3D Modeler)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

19 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09805
- https://helpx.adobe.com/security/products/substance3d-viewer/apsb25-72.html

Краткое описание: Выполнение произвольного кода в Microsoft SharePoint Enterprise Server, Microsoft Word, Microsoft Office, Microsoft SharePoint Server, 365 Apps for Enterprise, Microsoft Office for Mac

Идентификатор уязвимости: CVE-2025-53733
BDU:2025-09750

Идентификатор программной ошибки: CWE-681 Некорректное преобразование числовых типов

Уязвимый продукт: 2016 (Microsoft SharePoint Enterprise Server), 2016 (Microsoft Word), 2016 (Microsoft Word), 2019 (Microsoft Office), 2019 (Microsoft Office), 2019 (Microsoft SharePoint Server), - (365 Apps for Enterprise), - (365 Apps for Enterprise), LTSC 2021 (Microsoft Office), LTSC 2021 (Microsoft Office), LTSC 2021 (Microsoft Office for Mac), LTSC 2024 (Microsoft Office), LTSC 2024 (Microsoft Office), LTSC 2024 (Microsoft Office for Mac)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

20

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: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09750
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53733

21

Краткое описание: Выполнение произвольного кода в Windows

Идентификатор уязвимости: CVE-2025-53766
BDU:2025-09749

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

Уязвимый продукт: Server 2008 R2 SP1 (Windows), Server 2008 SP2 (Windows), Server 2008 SP2 (Windows), Server 2012 (Windows), Server 2012 R2 (Windows), 10 (Windows), 10 (Windows), 10 1607 (Windows), 10 1607 (Windows), Server 2016 (Windows), Server 2008 SP2 Server Core installation (Windows), Server 2008 SP2 Server Core installation (Windows), Server 2012 R2 Server Core installation (Windows), Server 2016 Server Core installation (Windows), Server 2008 R2 SP1 Server Core installation (Windows), Server 2012 Server Core installation (Windows), 10 1809 (Windows), 10 1809 (Windows), Server 2019 (Windows), Server 2019 Server Core installation (Windows), Server 2022 (Windows), Server 2022 Server Core installation (Windows), 10 21H2 (Windows), 10 21H2 (Windows), 10 21H2 (Windows), 11 22H2 (Windows), 11 22H2 (Windows), 10 22H2 (Windows), 10 22H2 (Windows), 10 22H2 (Windows), 11 23H2 (Windows), 11 23H2 (Windows), Server 2022 23H2 Edition Server Core installation (Windows), 11 24H2 (Windows), 11 24H2 (Windows), Server 2025 (Windows), Server 2025 Server Core installation (Windows)

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально созданного метафайла.

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: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09749
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53766

Краткое описание: Выполнение произвольного кода в 365 Apps for Enterprise, Microsoft Office, Microsoft Office for Mac

Идентификатор уязвимости: CVE-2025-53784
BDU:2025-09748

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: - (365 Apps for Enterprise), - (365 Apps for Enterprise), LTSC 2021 (Microsoft Office), LTSC 2021 (Microsoft Office), LTSC 2021 (Microsoft Office for Mac), LTSC 2024 (Microsoft Office), LTSC 2024 (Microsoft Office), LTSC 2024 (Microsoft Office for Mac)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

22 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09748
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53784

23

Краткое описание: Повышение привилегий в Windows

Идентификатор уязвимости: CVE-2025-53778
BDU:2025-09747

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Server 2008 R2 SP1 (Windows), Server 2008 SP2 (Windows), Server 2008 SP2 (Windows), Server 2012 (Windows), Server 2012 R2 (Windows), 10 (Windows), 10 (Windows), 10 1607 (Windows), 10 1607 (Windows), Server 2016 (Windows), Server 2008 SP2 Server Core installation (Windows), Server 2008 SP2 Server Core installation (Windows), Server 2012 R2 Server Core installation (Windows), Server 2016 Server Core installation (Windows), Server 2008 R2 SP1 Server Core installation (Windows), Server 2012 Server Core installation (Windows), 10 1809 (Windows), 10 1809 (Windows), Server 2019 (Windows), Server 2019 Server Core installation (Windows), Server 2022 (Windows), Server 2022 Server Core installation (Windows), 10 21H2 (Windows), 10 21H2 (Windows), 10 21H2 (Windows), 11 22H2 (Windows), 11 22H2 (Windows), 10 22H2 (Windows), 10 22H2 (Windows), 10 22H2 (Windows), 11 23H2 (Windows), 11 23H2 (Windows), Server 2022 23H2 Edition Server Core installation (Windows), 11 24H2 (Windows), 11 24H2 (Windows), Server 2025 (Windows), Server 2025 Server Core installation (Windows)

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Нарушение аутентификации.

Последствия эксплуатации: Повышение привилегий

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09747
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53778

Краткое описание: Потеря целостности в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23320
BDU:2025-09745

Идентификатор программной ошибки: CWE-209 Разглашение информации в сообщениях об ошибках

Уязвимый продукт: до 25.07 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Несанкционированный сбор информации.

Последствия эксплуатации: Потеря целостности

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

24

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09745
- https://nvidia.custhelp.com/app/answers/detail/a_id/5687

25

Краткое описание: Отказ в обслуживании в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23310
BDU:2025-09743

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: до 25.07 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

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: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09743
- https://nvidia.custhelp.com/app/answers/detail/a_id/5687
- https://www.cve.org/CVERecord?id=CVE-2025-23310"

Краткое описание: Отказ в обслуживании в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23331
BDU:2025-09741

Идентификатор программной ошибки: CWE-789 Неконтролируемое выделение памяти

Уязвимый продукт: до 25.06 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

26 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09741
- https://www.cve.org/CVERecord?id=CVE-2025-23331

Краткое описание: Отказ в обслуживании в Tenda AC20

Идентификатор уязвимости: CVE-2025-8810
BDU:2025-09738

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

Уязвимый продукт: 16.03.08.05 (Tenda AC20)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Чтение за пределами буфера.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

27

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-02 / 2025-08-02

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09738
- https://github.com/LaiwanHundun/CVE/blob/main/cve1
- https://vuldb.com/?submit.627394
- https://vuldb.com/?id.319339"

28

Краткое описание: Выполнение произвольного кода в Linksys RE6500, RE6250, RE6300, RE6350, RE7000, RE9000

Идентификатор уязвимости: CVE-2025-8816
BDU:2025-09737

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

Уязвимый продукт: 1.0.013.001 (RE6500), 1.0.04.001 (RE6250), 1.2.07.001 (RE6300), 1.0.04.001 (RE6350), 1.1.05.003 (RE7000), 1.0.04.002 (RE9000)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09737
- https://github.com/wudipjq/my_vuln/blob/main/Linksys1/vuln_50/50.md
- https://vuldb.com/?id.319350
- https://vuldb.com/?submit.626680"

29

Краткое описание: Выполнение произвольного кода в Linksys RE6500, RE6250, RE6300, RE6350, RE7000, RE9000

Идентификатор уязвимости: CVE-2025-8817
BDU:2025-09736

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

Уязвимый продукт: 1.0.013.001 (RE6500), 1.0.04.001 (RE6250), 1.2.07.001 (RE6300), 1.0.04.001 (RE6350), 1.1.05.003 (RE7000), 1.0.04.002 (RE9000)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09736
- https://github.com/wudipjq/my_vuln/blob/main/Linksys1/vuln_51/51.md
- https://vuldb.com/?submit.626681
- https://vuldb.com/?id.319351"

Краткое описание: Выполнение произвольного кода в Linksys RE6500, RE6250, RE6300, RE6350, RE7000, RE9000

Идентификатор уязвимости: CVE-2025-8819
BDU:2025-09735

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

Уязвимый продукт: 1.0.013.001 (RE6500), 1.0.04.001 (RE6250), 1.2.07.001 (RE6300), 1.0.04.001 (RE6350), 1.1.05.003 (RE7000), 1.0.04.002 (RE9000)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Выполнение произвольного кода

30

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09735
- https://github.com/wudipjq/my_vuln/blob/main/Linksys1/vuln_53/53.md
- https://vuldb.com/?submit.626683
- https://vuldb.com/?id.319353"

Краткое описание: Выполнение произвольного кода в IBM Tivoli Monitoring

Идентификатор уязвимости: CVE-2025-3320
BDU:2025-09698

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

Уязвимый продукт: от 6.3.0.7до 6.3.0.7 Service Pack 20 включительно (IBM Tivoli Monitoring)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Выполнение произвольного кода

31 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-05 / 2025-08-05

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09698
- https://www.ibm.com/support/pages/node/7241472

Краткое описание: Отказ в обслуживании в IBM Tivoli Monitoring

Идентификатор уязвимости: CVE-2025-3354
BDU:2025-09696

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

Уязвимый продукт: от 6.3.0.7до 6.3.0.7 Service Pack 20 включительно (IBM Tivoli Monitoring)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Отказ в обслуживании

32 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-05 / 2025-08-05

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09696
- https://www.ibm.com/support/pages/node/7241472

Краткое описание: Выполнение произвольного кода в Linksys RE6250, Linksys RE6500, Linksys RE6300, Linksys RE6350, Linksys RE7000, Linksys RE9000

Идентификатор уязвимости: CVE-2025-8832
BDU:2025-09695

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

Уязвимый продукт: 1.0.04.001 (Linksys RE6250), 1.0.013.001 (Linksys RE6500), 1.2.07.001 (Linksys RE6300), 1.0.04.001 (Linksys RE6350), 1.1.05.003 (Linksys RE7000), 1.0.04.002 (Linksys RE9000)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

33

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09695
- https://github.com/wudipjq/my_vuln/blob/main/Linksys1/vuln_48/48.md#poc
- https://vuldb.com/?ctiid.319366
- https://vuldb.com/?id.319366
- https://vuldb.com/?submit.626697
- https://www.linksys.com/"

34

Краткое описание: Выполнение произвольного кода в ThrottleStop

Идентификатор уязвимости: CVE-2025-7771
BDU:2025-09694

Идентификатор программной ошибки: CWE-782 Некорректное ограничение доступа к IOCTL

Уязвимый продукт: от 3.0.0.0 до 9.7.3 включительно (ThrottleStop)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного IOCTL-запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-06 / 2025-08-06

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09694
- https://github.com/klsecservices/Advisories/blob/master/K-TechPowerUp-2025-001.md
- https://securelist.com/av-killer-exploiting-throttlestop-sys/117026/"

Краткое описание: Потеря целостности в EcoStruxure Power Monitoring Expert, EcoStruxure PowerOperation (EPO) - Advanced Reporting and Dashboards Module

Идентификатор уязвимости: CVE-2025-54923
BDU:2025-09689

Идентификатор программной ошибки: CWE-502 Десериализация недоверенных данных

Уязвимый продукт: 2023 (EcoStruxure Power Monitoring Expert), 2024 R2 (EcoStruxure Power Monitoring Expert), 2024 (EcoStruxure Power Monitoring Expert), 2022 (EcoStruxure Power Monitoring Expert), 2022 w/ Advanced Reporting Module (EcoStruxure PowerOperation (EPO) - Advanced Reporting and Dashboards Module), 2024 w/ Advanced Reporting Module (EcoStruxure PowerOperation (EPO) - Advanced Reporting and Dashboards Module)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Потеря целостности

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09689
- https://www.se.com/ww/en/work/support/cybersecurity/security-notifications.jsp
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-224-03"

Краткое описание: Выполнение произвольного кода в Linksys RE6250, Linksys RE6500, Linksys RE6300, Linksys RE6350, Linksys RE7000, Linksys RE9000

Идентификатор уязвимости: CVE-2025-8831
BDU:2025-09678

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

Уязвимый продукт: 1.0.04.001 (Linksys RE6250), 1.0.013.001 (Linksys RE6500), 1.2.07.001 (Linksys RE6300), 1.0.04.001 (Linksys RE6350), 1.1.05.003 (Linksys RE7000), 1.0.04.002 (Linksys RE9000)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

36

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09678
- https://github.com/wudipjq/my_vuln/blob/main/Linksys1/vuln_47/47.md
- https://vuldb.com/?ctiid.319365
- https://vuldb.com/?id.319365
- https://vuldb.com/?submit.626696
- https://www.linksys.com/"

Краткое описание: Отказ в обслуживании в Linksys RE6250, Linksys RE6500, Linksys RE6300, Linksys RE6350, Linksys RE7000, Linksys RE9000

Идентификатор уязвимости: CVE-2025-8820
BDU:2025-09662

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

Уязвимый продукт: 1.0.04.001 (Linksys RE6250), 1.0.013.001 (Linksys RE6500), 1.2.07.001 (Linksys RE6300), 1.0.04.001 (Linksys RE6350), 1.1.05.003 (Linksys RE7000), 1.0.04.002 (Linksys RE9000)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Отказ в обслуживании

37 **Рекомендации по устранению:** Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09662
- https://github.com/wudipjq/my_vuln/blob/main/Linksys1/vuln_54/54.md#poc
- https://vuldb.com/?id.319354
- https://vuldb.com/?submit.626684"

Краткое описание: Отказ в обслуживании в Linksys RE6250, Linksys RE6500, Linksys RE6300, Linksys RE6350, Linksys RE7000, Linksys RE9000

Идентификатор уязвимости: CVE-2025-8824
BDU:2025-09661

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

Уязвимый продукт: 1.0.04.001 (Linksys RE6250), 1.0.013.001 (Linksys RE6500), 1.2.07.001 (Linksys RE6300), 1.0.04.001 (Linksys RE6350), 1.1.05.003 (Linksys RE7000), 1.0.04.002 (Linksys RE9000)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Запись за пределами буфера.

38 **Последствия эксплуатации:** Отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09661

Краткое описание: Отказ в обслуживании в Linksys RE6250, Linksys RE6500, Linksys RE6300, Linksys RE6350, Linksys RE7000, Linksys RE9000

Идентификатор уязвимости: CVE-2025-8822
BDU:2025-09659

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

Уязвимый продукт: 1.0.04.001 (Linksys RE6250), 1.0.013.001 (Linksys RE6500), 1.2.07.001 (Linksys RE6300), 1.0.04.001 (Linksys RE6350), 1.1.05.003 (Linksys RE7000), 1.0.04.002 (Linksys RE9000)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Отказ в обслуживании

39 **Рекомендации по устранению:** Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09659
- https://vuldb.com/?submit.626686
- https://vuldb.com/?id.319356
- https://github.com/wudipjq/my_vuln/blob/main/Linksys1/vuln_56/56.md#poc"

40

Краткое описание: Отказ в обслуживании в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23322
BDU:2025-09656

Идентификатор программной ошибки: CWE-415 Двойное освобождение

Уязвимый продукт: до 25.05 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09656

41

Краткое описание: Отказ в обслуживании в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23318
BDU:2025-09655

Идентификатор программной ошибки: CWE-805 Доступ к памяти за пределами буфера

Уязвимый продукт: до 25.05 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

Последствия эксплуатации: Отказ в обслуживании

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09655

42

Краткое описание: Отказ в обслуживании в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23311
BDU:2025-09654

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: до 25.05 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Переполнение буфера.

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: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09654
- https://nvidia.custhelp.com/app/answers/detail/a_id/5687
- https://www.cve.org/CVERecord?id=CVE-2025-23311"

43

Краткое описание: Отказ в обслуживании в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23324
BDU:2025-09653

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

Уязвимый продукт: до 25.05 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09653
- https://nvidia.custhelp.com/app/answers/detail/a_id/5687
- https://www.cve.org/CVERecord?id=CVE-2025-23325"

44

Краткое описание: Отказ в обслуживании в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23321
BDU:2025-09652

Идентификатор программной ошибки: CWE-369 Деление на ноль

Уязвимый продукт: до 25.07 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного 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: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09652
- https://nvidia.custhelp.com/app/answers/detail/a_id/5687
- https://www.cve.org/CVERecord?id=CVE-2025-23321"

45

Краткое описание: Отказ в обслуживании в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23327
BDU:2025-09651

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

Уязвимый продукт: до 25.05 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09651
- https://nvidia.custhelp.com/app/answers/detail/a_id/5687
- https://www.cve.org/CVERecord?id=CVE-2025-23327"

Краткое описание: Отказ в обслуживании в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23325
BDU:2025-09650

Идентификатор программной ошибки: CWE-674 Неконтролируемая рекурсия

Уязвимый продукт: до 25.05 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

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.

46

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09650
- https://nvidia.custhelp.com/app/answers/detail/a_id/5687
- https://www.cve.org/CVERecord?id=CVE-2025-23325"

47

Краткое описание: Выполнение произвольного кода в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23317
BDU:2025-09649

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

Уязвимый продукт: до 25.07 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного HTTP-запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09649
- https://nvidia.custhelp.com/app/answers/detail/a_id/5687
- https://www.cve.org/CVERecord?id=CVE-2025-23317"

Краткое описание: Отказ в обслуживании в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23326
BDU:2025-09648

Идентификатор программной ошибки: CWE-690 Отсутствие проверки возвращаемого значения, приводящее к разыменованию нулевого указателя

Уязвимый продукт: до 25.05 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

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.

48

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09648
- https://nvidia.custhelp.com/app/answers/detail/a_id/5687
- https://www.cve.org/CVERecord?id=CVE-2025-23326"

49

Краткое описание: Отказ в обслуживании в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23323
BDU:2025-09647

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

Уязвимый продукт: до 25.05 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09647
- https://nvidia.custhelp.com/app/answers/detail/a_id/5687
- https://www.cve.org/CVERecord?id=CVE-2025-23323"

Краткое описание: Повышение привилегий в Azure Open AI

Идентификатор уязвимости: CVE-2025-53767
BDU:2025-09637

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

Уязвимый продукт: - (Azure Open AI)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

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.

50

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-07 / 2025-08-07

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09637
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53767

Краткое описание: Выполнение произвольного кода в Apex One

Идентификатор уязвимости: CVE-2025-54987
BDU:2025-09573

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

Уязвимый продукт: 2019 (Apex One)

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Инъекция.

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.

51

Оценка CVSSv3: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09573
- https://success.trendmicro.com/en-US/solution/KA-0020652
- https://www.zerodayinitiative.com/advisories/ZDI-25-772/"

52

Краткое описание: Выполнение произвольного кода в Linksys RE6250, Linksys RE6500, Linksys RE6300, Linksys RE6350, Linksys RE7000, Linksys RE9000

Идентификатор уязвимости: CVE-2025-8826
BDU:2025-09594

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

Уязвимый продукт: 1.0.04.001 (Linksys RE6250), 1.0.013.001 (Linksys RE6500), 1.2.07.001 (Linksys RE6300), 1.0.04.001 (Linksys RE6350), 1.1.05.003 (Linksys RE7000), 1.0.04.002 (Linksys RE9000)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Отправка специально созданного POST-запроса.

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09594
- https://github.com/wudipjq/my_vuln/blob/main/Linksys1/vuln_42/42.md#poc

Краткое описание: Повышение привилегий в Vault Enterprise, Vault Community Edition

Идентификатор уязвимости: CVE-2025-5999
BDU:2025-09565

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

Уязвимый продукт: до 1.18.11 (Vault Enterprise), до 1.16.22 (Vault Enterprise), от 0.10.4 до 1.20.0 (Vault Community Edition), от 0.10.4 до 1.20.0 (Vault Enterprise), до 1.19.6 (Vault Enterprise)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

Последствия эксплуатации: Повышение привилегий

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

Оценка CVSSv3: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09565
- https://discuss.hashicorp.com/t/hcsec-2025-13-vault-root-namespace-operator-may-elevate-token-privileges/76032

Краткое описание: Повышение привилегий в Dell SupportAssist OS Recovery

Идентификатор уязвимости: CVE-2025-38747
BDU:2025-09593

Идентификатор программной ошибки: CWE-378 Создание временных файлов с небезопасными разрешениями

Уязвимый продукт: до 5.5.14.0 (Dell SupportAssist OS Recovery)

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Нарушение авторизации.

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.

54

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-06 / 2025-08-06

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09593
- https://www.dell.com/support/kbdoc/en-us/000353093/dsa-2025-315

Краткое описание: Потеря целостности в HarmonyOS

Идентификатор уязвимости: CVE-2025-54627
BDU:2025-09592

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: 5.1.0 (HarmonyOS), 5.0.1 (HarmonyOS)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Запись за пределами буфера.

Последствия эксплуатации: Потеря целостности

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-05 / 2025-08-05

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09592
- https://consumer.huawei.com/en/support/bulletin/2025/8/

Краткое описание: Выполнение произвольного кода в SATO CL4NX Plus, SATO CL4NX-J Plus, SATO CL6NX Plus, SATO CL6NX-J Plus

Идентификатор уязвимости: CVE-2025-22470
BDU:2025-09584

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

Уязвимый продукт: до 1.15.5-r1 (SATO CL4NX Plus), до 1.15.5-r1 (SATO CL4NX-J Plus), до 1.15.5-r1 (SATO CL6NX Plus), до 1.15.5-r1 (SATO CL6NX-J Plus)

Категория уязвимого продукта: Программно-аппаратное решение

Способ эксплуатации: Не определено

Последствия эксплуатации: Выполнение произвольного кода

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

56

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09584
- https://www.sato-global.com/support_notices/240830/
- https://jvn.jp/en/jp/JVN16547726/"

57

Краткое описание: Повышение привилегий в Cloud Connect Advanced (CCA)

Идентификатор уязвимости: CVE-2025-7768
BDU:2025-09580

Идентификатор программной ошибки: CWE-798 Использование жестко закодированных учетных данных

Уязвимый продукт: до 4.0.1 включительно (Cloud Connect Advanced (CCA))

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Повышение привилегий

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-05 / 2025-08-05

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09580
- https://www.tigoenergy.com/product/cloud-connect-advanced
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-217-02"

Краткое описание: Повышение привилегий в Cloud Connect Advanced (CCA)

Идентификатор уязвимости: CVE-2025-7769
BDU:2025-09579

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

Уязвимый продукт: до 4.0.1 включительно (Cloud Connect Advanced (CCA))

Категория уязвимого продукта: Не определено

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Повышение привилегий

58 **Рекомендации по устранению:** Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-05 / 2025-08-05

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09579
- https://www.tigoenergy.com/product/cloud-connect-advanced
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-217-02"

59

Краткое описание: Потеря целостности в Cloud Connect Advanced (CCA)

Идентификатор уязвимости: CVE-2025-7770
BDU:2025-09578

Идентификатор программной ошибки: CWE-337 Предсказуемое начальное значение ГПСЧ

Уязвимый продукт: до 4.0.1 включительно (Cloud Connect Advanced (CCA))

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Потеря целостности

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-05 / 2025-08-05

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09578
- https://www.tigoenergy.com/product/cloud-connect-advanced
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-217-02"

Краткое описание: Выполнение произвольного кода в Apex One

Идентификатор уязвимости: CVE-2025-54987
BDU:2025-09573

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

Уязвимый продукт: 2019 (Apex One)

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Инъекция.

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.

60

Оценка CVSSv3: 9.4 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09573
- https://success.trendmicro.com/en-US/solution/KA-0020652
- https://www.zerodayinitiative.com/advisories/ZDI-25-772/"

61

Краткое описание: Повышение привилегий в Vault Enterprise, Vault Community Edition

Идентификатор уязвимости: CVE-2025-5999
BDU:2025-09565

Идентификатор программной ошибки: CWE-266 Некорректное назначение привилегий

Уязвимый продукт: до 1.18.11 (Vault Enterprise), до 1.16.22 (Vault Enterprise), от 0.10.4 до 1.20.0 (Vault Community Edition), от 0.10.4 до 1.20.0 (Vault Enterprise), до 1.19.6 (Vault Enterprise)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Нарушение авторизации.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09565
- https://discuss.hashicorp.com/t/hcsec-2025-13-vault-root-namespace-operator-may-elevate-token-privileges/76032

62

Краткое описание: Выполнение произвольного кода в Vault Enterprise, Vault Community Edition

Идентификатор уязвимости: CVE-2025-6000
BDU:2025-09562

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

Уязвимый продукт: до 1.19.7 (Vault Enterprise), до 1.18.12 (Vault Enterprise), до 1.16.23 (Vault Enterprise), от 0.8.0 до 1.20.1 (Vault Community Edition), от 0.8.0 до 1.20.1 (Vault Enterprise)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Инъекция.

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09562
- https://discuss.hashicorp.com/t/hcsec-2025-14-privileged-vault-operator-may-execute-code-on-the-underlying-host/76033

63

Краткое описание: Потеря целостности в JSON Web Encryption (JWE)

Идентификатор уязвимости: CVE-2025-54887
BDU:2025-09559

Идентификатор программной ошибки: CWE-354 Некорректная проверка контрольных сумм

Уязвимый продукт: до 1.1.1 (JSON Web Encryption (JWE))

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Подмена при взаимодействии.

Последствия эксплуатации: Потеря целостности

Рекомендации по устранению: Данная уязвимость устраняется официальным патчем вендора. 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: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-07 / 2025-08-07

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09559
- https://github.com/jwt/ruby-jwe/commit/1e719d79ba3d7aadaa39a2f08c25df077a0f9ff1
- https://github.com/jwt/ruby-jwe/security/advisories/GHSA-c7p4-hx26-pr73"

64

Краткое описание: Чтение локальных файлов в Adobe Experience Manager (AEM) Forms on JEE

Идентификатор уязвимости: CVE-2025-54254
BDU:2025-09480

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

Уязвимый продукт: до 6.5.0-0108 (Adobe Experience Manager (AEM) Forms on JEE)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного XML-кода.

Последствия эксплуатации: Чтение локальных файлов

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-05 / 2025-08-05

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09480
- https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html

Краткое описание: Потеря целостности в HarmonyOS

Идентификатор уязвимости: CVE-2025-54634
BDU:2025-09453

Идентификатор программной ошибки: CWE-755 Некорректная обработка исключений

Уязвимый продукт: 5.1.0 (HarmonyOS), 5.0.1 (HarmonyOS)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

Последствия эксплуатации: Потеря целостности

65 **Рекомендации по устранению:** Данная уязвимость устраняется официальным патчем вендора. 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:L/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-05 / 2025-08-05

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09453
- https://consumer.huawei.com/en/support/bulletin/2025/8/

66

Краткое описание: Выполнение произвольного кода в Arena Simulation

Идентификатор уязвимости: CVE-2025-7025
BDU:2025-09444

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

Уязвимый продукт: до 16.20.10 (Arena Simulation)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Переполнение буфера.

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: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-08-05 / 2025-08-05

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09444
- https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1731.html

67

Краткое описание: Выполнение произвольного кода в NVIDIA Triton Inference Server

Идентификатор уязвимости: CVE-2025-23319
BDU:2025-09443

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

Уязвимый продукт: до 25.07 (NVIDIA Triton Inference Server)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированного запроса.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-04 / 2025-08-04

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09443
- https://nvidia.custhelp.com/app/answers/detail/a_id/5687
- https://www.wiz.io/blog/nvidia-triton-cve-2025-23319-vuln-chain-to-ai-server"

68

Краткое описание: Выполнение произвольного кода в Adobe Experience Manager (AEM) Forms on JEE

Идентификатор уязвимости: CVE-2025-54253
BDU:2025-09420

Идентификатор программной ошибки: CWE-16 Уязвимости, связанные с конфигурацией

Уязвимый продукт: до 6.5.0-0108 (Adobe Experience Manager (AEM) Forms on JEE)

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-05 / 2025-08-05

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09420
- https://helpx.adobe.com/security/products/aem-forms/apsb25-82.html

Краткое описание: Выполнение произвольного кода в Android

Идентификатор уязвимости: CVE-2025-48530
BDU:2025-09417

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: Android (16)

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Нарушение авторизации.

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.

69

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

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09417
- https://source.android.com/docs/security/bulletin/2025-08-01?hl=ru
- https://www.anti-malware.ru/news/2025-08-05-111332/46888
- https://cyberscoop.com/android-security-update-august-2025/"

Краткое описание: Повышение привилегий в Android

Идентификатор уязвимости: CVE-2025-22441
BDU:2025-09416

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: Android (13), Android (14), Android (15)

Категория уязвимого продукта: Unix-подобные операционные системы и их компоненты

Способ эксплуатации: Не определено

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.

70

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09416
- https://source.android.com/docs/security/bulletin/2025-08-01?hl=ru
- https://www.anti-malware.ru/news/2025-08-05-111332/46888
- https://cyberscoop.com/android-security-update-august-2025/"

Краткое описание: Повышение привилегий в Android

Идентификатор уязвимости: CVE-2025-48533
BDU:2025-09415

Идентификатор программной ошибки: CWE-264 Уязвимость в управлении доступом, привилегиями и разрешениями

Уязвимый продукт: 13 (Android), 14 (Android), 15 (Android), 16 (Android)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

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.

71

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09415
- https://source.android.com/docs/security/bulletin/2025-08-01?hl=ru
- https://www.anti-malware.ru/news/2025-08-05-111332/46888
- https://cyberscoop.com/android-security-update-august-2025/"

Краткое описание: Выполнение произвольного кода в NVIDIA Corp.

Идентификатор уязвимости: CVE-2025-23276
BDU:2025-09389

Идентификатор программной ошибки: CWE-552 Непредусмотренный доступ к файлам или каталогам

Уязвимый продукт: до 573.48 (NVIDIA RTX R570), до 577.00 (GeForce R575), до 539.41 (NVIDIA RTX R570), до 573.48 (Quadro R570), до 539.41 (Quadro R535), до 573.48 (NVIDIA NVS R570), до 539.41 (NVIDIA NVS R535), до 573.48 (Tesla R570), до 539.41 (Tesla R535)

Категория уязвимого продукта: Не определено

Способ эксплуатации: Несанкционированный сбор информации.

72

Последствия эксплуатации: Выполнение произвольного кода

Рекомендации по устранению: Принять меры по уменьшению уровня опасности, указанные на официальном сайте вендора.

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-02 / 2025-08-02

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09389
- https://nvidia.custhelp.com/app/answers/detail/a_id/5670

Краткое описание: Выполнение произвольного кода в Squid Software Foundation

Идентификатор уязвимости: CVE-2025-54574
BDU:2025-09345

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

Уязвимый продукт: Squid: до 6.4

Категория уязвимого продукта: Не определено

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.

73

Оценка CVSSv3: 9.3 AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-01 / 2025-08-01

Ссылки на источник:

- https://bdu.fstec.ru/vul/2025-09345
- https://github.com/squid-cache/squid/releases/tag/SQUID_6_4

Краткое описание: Выполнение произвольного кода в Fortinet products

Идентификатор уязвимости: CVE-2024-26009
BDU:2025-09924

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

Уязвимый продукт: FortiOS: 6.0
FortiPAM: 1.0
FortiPAM: 1.2
FortiPAM: 1.1
FortiOS: от 6.4.0 до 6.4.16
FortiProxy: от 7.0.0 до 7.0.16
FortiOS: от 6.2.0 до 6.2.17
FortiProxy: от 7.4.0 до 7.4.3
FortiProxy: от 7.2.0 до 7.2.9
FortiSwitchManager: от 7.2.0 до 7.2.4
FortiSwitchManager: от 7.0.0 до 7.0.4

74

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Нарушение 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: 8.1 AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-12 / 2025-08-12

Ссылки на источник:

- https://fortiguard.fortinet.com/psirt/FG-IR-24-042

- https://bdu.fstec.ru/vul/2025-09924
- https://bdu.fstec.ru/vul/2025-09924

Краткое описание: Выполнение произвольного кода в Rockwell Automation

Идентификатор уязвимости: CVE-2025-7353
BDU:2025-09996

Идентификатор программной ошибки: CWE-1188 Инициализация ресурса с небезопасными параметрами по умолчанию

Уязвимый продукт: 1756-EN2TP Series A: до 12.001
1756-EN3TR Series B: до 12.001
1756-EN2TR Series C: до 12.001
1756-EN2F Series C: до 12.001
1756-EN2T Series D: до 12.001

Категория уязвимого продукта: Не определено

Способ эксплуатации: Не определено

75

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: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-14 / 2025-08-14

Ссылки на источник:

- https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1732.html
- https://bdu.fstec.ru/vul/2025-09996

Краткое описание: Отказ в обслуживании в Elastic NV

Идентификатор уязвимости: BDU:2025-09997

Идентификатор программной ошибки: CWE-476 Разыменование нулевого указателя

Уязвимый продукт: Elastic Endpoint Detection and Response (EDR): 8.17.6

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Не определено

Последствия эксплуатации: Отказ в обслуживании

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

76

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

Оценка CVSSv4: Не определено

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-08-18 / 2025-08-18

Ссылки на источник:

- https://ashes-cybersecurity.com/0-day-research/
- https://bdu.fstec.ru/vul/2025-09997