НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-09-29.1 | 29 сентября 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2025-20363	Cisco IOS XE	Сетевой	ACE	2025-09-25	✓
2	Критическая	CVE-2025-20333	Cisco ASA and FTD	Сетевой	ACE	2025-09-25	✓
3	Высокая	CVE-2025-20327	Cisco IOS Software	Сетевой	DoS	2025-09-25	✓
4	Критическая	CVE-2025-9321	WPCasa pluugin for WordPress	Сетевой	ACE	2025-09-25	✓
5	Высокая	CVE-2025-20334	Cisco IOS XE Software	Сетевой	ACE	2025-09-25	✓
6	Высокая	CVE-2025-20315	Cisco IOS XE Software	Сетевой	DoS	2025-09-25	✓
7	Критическая	CVE-2025-10925	Gimp	Сетевой	ACE	2025-09-25	✓
8	Высокая	CVE-2025-10924	Gimp	Локальный	ACE	2025-09-25	✓
9	Высокая	CVE-2025-10923	Gimp	Локальный	ACE	2025-09-25	✓
10	Высокая	CVE-2025-10922	Gimp	Локальный	ACE	2025-09-25	✓
11	Критическая	CVE-2025-10921	Gimp	Сетевой	ACE	2025-09-25	✓
12	Высокая	CVE-2025-10920	Gimp	Локальный	ACE	2025-09-25	✓
13	Высокая	CVE-2025-59251	Microsoft Edge	Сетевой	ACE	2025-09-24	✓

14	Высокая	CVE-2025-20352	Cisco IOS and IOS XE SNMP implementation	Сетевой	ACE	2025-09-24	✓
15	Высокая	CVE-2025-8354	Autodesk Revit	Локальный	ACE	2025-09-24	✓
16	Высокая	CVE-2025-9449	Dassault Systmes eDrawings	Локальный	ACE	2025-09-23	✓
17	Высокая	CVE-2025-9447	Dassault Systmes eDrawings	Локальный	OSI	2025-09-23	✓
18	Высокая	CVE-2025-9450	Dassault Systmes eDrawings	Локальный	ACE	2025-09-23	✓
19	Высокая	CVE-2025-10200	Google ChromeOS LTS	Сетевой	ACE	2025-09-22	✓
20	Критическая	CVE-2025-40600	SonicOS SSL VPN	Сетевой	DoS	2025-07-30	✓
21	Критическая	CVE-2025-40599	SonicWall SMA100 SSL-VPN	Сетевой	WLF	2025-07-23	✓
22	Высокая	CVE-2025-40597	SonicWall SMA100 SSL-VPN	Сетевой	ACE	2025-07-23	✓

1

Краткое описание: Выполнение произвольного кода в Cisco IOS XE

Идентификатор уязвимости: CVE-2025-20363
BDU:2025-11752

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

Уязвимый продукт: Cisco IOS XE: до 16.12.14, 17.9.7a, 17.9.8, 17.12.6, 17.15.1z, 17.15.3a, 17.15.4, 17.18.1

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Оценка CVSSv4: 7.2 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-25 / 2025-09-25

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http-code-exec-WmfP3h3O
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwo35704
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwo35779
- https://bdu.fstec.ru/vul/2025-11752

2

Краткое описание: Выполнение произвольного кода в Cisco ASA and FTD

Идентификатор уязвимости: CVE-2025-20333
BDU:2025-11706

Идентификатор программной ошибки: CWE-120 Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)

Уязвимый продукт: Cisco Adaptive Security Appliance (ASA): до 9.16.4.85, 9.17.1.45, 9.18.4.47, 9.19.1.37, 9.20.3.7, 9.22.1.3
Cisco Firewall Threat Defense (FTD): до 7.0.8.1, 7.2.9, 7.4.2.4

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально созданных HTTP-запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: 8.7 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-25 / 2025-09-25

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwq79831
- https://bdu.fstec.ru/vul/2025-11706

Краткое описание: Отказ в обслуживании в Cisco IOS Software

Идентификатор уязвимости: CVE-2025-20327
BDU:2025-11723

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Cisco IOS: все версии
Cisco IE 2000 Series: все версии
Cisco IE 3010 Series: все версии
Cisco IE 4000 Series: все версии
Cisco IE 4010 Series: все версии
Cisco IE 5000 Series: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

3 **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: 7.7 AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-25 / 2025-09-25

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-invalid-url-dos-Nvxszf6u
- https://bdu.fstec.ru/vul/2025-11723

4

Краткое описание: Выполнение произвольного кода в WPCasa pluugin for WordPress

Идентификатор уязвимости: CVE-2025-9321

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

Уязвимый продукт: WPCasa: 1.4.0 - 1.4.1

Категория уязвимого продукта: Универсальные компоненты и библиотеки

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-25 / 2025-09-25

Ссылки на источник:

- https://plugins.trac.wordpress.org/browser/wpcasa/trunk/includes/class-wpsight-api.php#L48
- https://plugins.trac.wordpress.org/changeset/3365172/
- https://www.wordfence.com/threat-intel/vulnerabilities/id/c1001b2b-395a-44ee-827e-6e57f7a50218?source=cve

5

Краткое описание: Выполнение произвольного кода в Cisco IOS XE Software

Идентификатор уязвимости: CVE-2025-20334
BDU:2025-11724

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

Уязвимый продукт: Cisco IOS XE: 17.12.4

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-25 / 2025-09-25

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-xe-cmd-inject-rPJM8BGL
- https://bdu.fstec.ru/vul/2025-11724

6

Краткое описание: Отказ в обслуживании в Cisco IOS XE Software

Идентификатор уязвимости: CVE-2025-20315
BDU:2025-11722

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

Уязвимый продукт: Cisco IOS XE: 17.3.7
1100 Integrated Services Routers: все версии
4000 Series Integrated Services Routers: все версии
ASR 920 Series Aggregation Services Routers: все версии
ASR 1000 Series Aggregation Services Routers: все версии
Catalyst 1101 Rugged Routers: все версии
Catalyst 8000V Edge Software: все версии
Catalyst 8200 Series Edge Platforms: все версии
Catalyst 8300 Series Edge Platforms: все версии
Catalyst 8500 Edge Platforms: все версии
Catalyst 8500L Edge Platforms: все версии
Catalyst IR8300 Rugged Series Routers: все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-25 / 2025-09-25

Ссылки на источник:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nbar-dos-LAvwTmeT
- https://bdu.fstec.ru/vul/2025-11722

7

Краткое описание: Выполнение произвольного кода в Gimp

Идентификатор уязвимости: CVE-2025-10925

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Gimp: 3.0.0 - 3.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-25 / 2025-09-25

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-914/
- https://gitlab.gnome.org/GNOME/gimp/-/merge_requests/2450
- https://gitlab.gnome.org/GNOME/gimp/-/commit/002b22c15028b18557bd0823a081af9ed5316679
- https://gitlab.gnome.org/GNOME/gimp/-/issues/14816

8

Краткое описание: Выполнение произвольного кода в Gimp

Идентификатор уязвимости: CVE-2025-10924

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

Уязвимый продукт: Gimp: 3.0.0 - 3.1.4

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-25 / 2025-09-25

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-913/
- https://gitlab.gnome.org/GNOME/gimp/-/commit/53b18653bca9404efeab953e75960b1cf7dedbed
- https://gitlab.gnome.org/GNOME/gimp/-/merge_requests/2448
- https://gitlab.gnome.org/GNOME/gimp/-/issues/14813

Краткое описание: Выполнение произвольного кода в Gimp

Идентификатор уязвимости: CVE-2025-10923

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

Уязвимый продукт: Gimp: 3.0.0 - 3.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

9

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-25 / 2025-09-25

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-912/
- https://gitlab.gnome.org/GNOME/gimp/-/commit/2d2d39f3da1d0b01ca7d71ad2b7a8725ee92ed96
- https://gitlab.gnome.org/GNOME/gimp/-/issues/14812

Краткое описание: Выполнение произвольного кода в Gimp

Идентификатор уязвимости: CVE-2025-10922

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

Уязвимый продукт: Gimp: 3.0.0 - 3.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

10

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-25 / 2025-09-25

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-911/
- https://gitlab.gnome.org/GNOME/gimp/-/commit/3d909166463731e94dfe62042d76225ecfc4c1e4
- https://gitlab.gnome.org/GNOME/gimp/-/issues/14811

Краткое описание: Выполнение произвольного кода в Gimp

Идентификатор уязвимости: CVE-2025-10921

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

Уязвимый продукт: Gimp: 3.0.0 - 3.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

11

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-25 / 2025-09-25

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-910/
- https://gitlab.gnome.org/GNOME/gegl/-/commit/0e68b7471dabf2800d780819c19bd5e6462f565f
- https://gitlab.gnome.org/GNOME/gegl/-/issues/430

12

Краткое описание: Выполнение произвольного кода в Gimp

Идентификатор уязвимости: CVE-2025-10920

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Gimp: 3.0.0 - 3.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-25 / 2025-09-25

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-909/
- https://gitlab.gnome.org/GNOME/gimp/-/merge_requests/2443
- https://gitlab.gnome.org/GNOME/gimp/-/commit/5f4329d324b0db7a857918941ef7e1d27f3d3992
- https://gitlab.gnome.org/GNOME/gimp/-/issues/14818

13

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2025-59251

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Microsoft Edge: 100.0.1185.29 - 140.0.3485.71

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 7.6 AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:L

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-24 / 2025-09-24

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-59251

Краткое описание: Выполнение произвольного кода в Cisco IOS and IOS XE SNMP implementation

Идентификатор уязвимости: CVE-2025-20352

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Cisco IOS XE:
17.12 - 17.12.5c

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

14

Оценка CVSSv3: 7.7 AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H

Оценка CVSSv4: 8.7 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-09-24 / 2025-09-24

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-x4LPhte
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwq31287

Краткое описание: Выполнение произвольного кода в Autodesk Revit

Идентификатор уязвимости: CVE-2025-8354

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

Уязвимый продукт: Revit:
2026 - 2026.2

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

15

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-24 / 2025-09-24

Ссылки на источник:

- https://www.autodesk.com/trust/security-advisories/adsk-sa-2025-0021
- https://www.zerodayinitiative.com/advisories/ZDI-25-907/

Краткое описание: Выполнение произвольного кода в Dassault Systmes eDrawings

Идентификатор уязвимости: CVE-2025-9449

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: eDrawings:
SOLIDWORKS Desktop 2025

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

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

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-23 / 2025-09-23

Ссылки на источник:

- https://www.3ds.com/trust-center/security/security-advisories/cve-2025-9449
- https://www.zerodayinitiative.com/advisories/ZDI-25-903/

17

Краткое описание: Получение конфиденциальной информации в Dassault Systmes eDrawings

Идентификатор уязвимости: CVE-2025-9447

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: eDrawings:
SOLIDWORKS Desktop 2025

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-23 / 2025-09-23

Ссылки на источник:

- https://www.3ds.com/trust-center/security/security-advisories/cve-2025-9447
- https://www.zerodayinitiative.com/advisories/ZDI-25-904/

Краткое описание: Выполнение произвольного кода в Dassault Systmes eDrawings

Идентификатор уязвимости: CVE-2025-9450

Идентификатор программной ошибки: CWE-457 Использование неинициализированной переменной

Уязвимый продукт: eDrawings:
SOLIDWORKS Desktop 2025

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

18

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-23 / 2025-09-23

Ссылки на источник:

- https://www.3ds.com/trust-center/security/security-advisories/cve-2025-9450
- https://www.zerodayinitiative.com/advisories/ZDI-25-902/

19

Краткое описание: Выполнение произвольного кода в Google ChromeOS LTS

Идентификатор уязвимости: CVE-2025-10200
BDU:2025-11244

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Chrome OS:
до 132.0.6834.244

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2025-09-22 / 2025-09-22

Ссылки на источник:

- https://chromereleases.googleblog.com/2025/09/long-term-support-channel-update-for_19.html
- https://bdu.fstec.ru/vul/2025-11244

20

Краткое описание: Отказ в обслуживании в SonicOS SSL VPN

Идентификатор уязвимости: CVE-2025-40600

Идентификатор программной ошибки: CWE-134 Использование форматной строки, контролируемой извне

Уязвимый продукт: SonicOS: до 7.3.0-7012

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-30 / 2025-07-30

Ссылки на источник:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0013

Краткое описание: Запись локальных файлов в SonicWall SMA100 SSL-VPN

Идентификатор уязвимости: CVE-2025-40599
BDU:2025-10717

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

Уязвимый продукт: SMA 100: 10.2.0.2-20sv - 10.2.1.15-81sv

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Запись локальных файлов

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

21

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-23 / 2025-07-23

Ссылки на источник:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0014
- https://bdu.fstec.ru/vul/2025-10717

Краткое описание: Выполнение произвольного кода в SonicWall SMA100 SSL-VPN

Идентификатор уязвимости: CVE-2025-40597
BDU:2025-10714

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

Уязвимый продукт: SMA 100: 10.2.0.2-20sv - 10.2.1.15-81sv

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданных запросов.

Последствия эксплуатации: Выполнение произвольного кода

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

22

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-07-23 / 2025-07-23

Ссылки на источник:

- https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0012
- https://bdu.fstec.ru/vul/2025-10714