НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2026-01-19.1 | 19 января 2026 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2026-0881	Mozilla Thunderbird	Сетевой	ACE	2026-01-15	✓
2	Критическая	CVE-2026-0884	Mozilla Thunderbird	Сетевой	DoS	2026-01-15	✓
3	Высокая	CVE-2026-0889	Mozilla Thunderbird	Сетевой	DoS	2026-01-15	✓
4	Критическая	CVE-2026-0892	Mozilla Thunderbird	Сетевой	ACE	2026-01-15	✓
5	Высокая	CVE-2026-0891	Mozilla Thunderbird и Thunderbird ESR	Сетевой	ACE	2026-01-15	✓
6	Критическая	CVE-2026-0884	Mozilla Thunderbird ESR	Сетевой	DoS	2026-01-15	✓
7	Высокая	CVE-2025-14327	Mozilla Thunderbird ESR	Сетевой	OSI	2026-01-15	✓
8	Высокая	CVE-2026-0882	Mozilla Thunderbird и Thunderbird ESR	Сетевой	ACE	2026-01-15	✓
9	Высокая	CVE-2026-0880	Mozilla Thunderbird и Thunderbird ESR	Сетевой	ACE	2026-01-15	✓
10	Критическая	CVE-2026-0879	Mozilla Thunderbird и Thunderbird ESR	Сетевой	ACE	2026-01-15	✓
11	Высокая	CVE-2026-0878	Mozilla Thunderbird и Thunderbird ESR	Сетевой	ACE	2026-01-15	✓
12	Высокая	CVE-2026-0877	Mozilla Thunderbird и Thunderbird ESR	Сетевой	ACE	2026-01-15	✓
13	Высокая	CVE-2026-21287	Adobe Substance 3D Stager	Локальный	ACE	2026-01-15	✓

14	Высокая	CVE-2026-21305	Adobe Substance 3D Painter	Локальный	ACE	2026-01-15	✓
15	Высокая	CVE-2026-21306	Adobe Substance 3D Sampler	Локальный	ACE	2026-01-15	✓
16	Высокая	CVE-2026-21283	Adobe Bridge	Локальный	ACE	2026-01-15	✓
17	Высокая	CVE-2026-21280	Adobe Illustrator	Локальный	ACE	2026-01-15	✓
18	Высокая	CVE-2026-21281	Adobe InCopy	Локальный	ACE	2026-01-15	✓
19	Высокая	CVE-2026-21304	Adobe InDesign	Локальный	ACE	2026-01-15	✓
20	Высокая	CVE-2026-21277	Adobe InDesign	Локальный	ACE	2026-01-15	✓
21	Высокая	CVE-2026-21276	Adobe InDesign	Локальный	ACE	2026-01-15	✓
22	Высокая	CVE-2026-21275	Adobe InDesign	Локальный	ACE	2026-01-15	✓
23	Критическая	CVE-2026-21858	n8n	Сетевой	OSI	2026-01-07	✓
24	Критическая	CVE-2025-68613	n8n	Сетевой	OSI	2025-12-23	✓
25	Критическая	CVE-2025-68668	n8n	Сетевой	ACE	2026-01-07	✓
26	Критическая	CVE-2025-20393	Cisco Secure Email Gateway And Cisco Secure Email and Web Manager	Сетевой	ACE	2025-12-17	✗
27	Критическая	CVE-2025-14733	WatchGuard Firebox iked	Сетевой	ACE	2025-12-19	✓
28	Высокая	CVE-2025-15059	GIMP	Локальный	ACE	2026-01-12	✓

29	Критическая	CVE-2025-66589	AzeoTech DAQFactory	Сетевой	OSI	2026-01-09	✓
30	Высокая	CVE-2025-66585	AzeoTech DAQFactory	Локальный	ACE	2026-01-09	✓
31	Высокая	CVE-2025-66586	AzeoTech DAQFactory	Локальный	ACE	2026-01-09	✓
32	Критическая	CVE-2025-66590	AzeoTech DAQFactory	Сетевой	ACE	2026-01-09	✓
33	Не определено	CVE-2025-65606	TOTOLINK EX200	Не определено	ACE	2026-01-08	✗
34	Высокая	CVE-2025-69194	GNU wget	Сетевой	OSI	2026-01-07	✓
35	Высокая	CVE-2026-0628	Google Chrome и Microsoft Edge	Сетевой	SB	2026-01-06	✓
36	Высокая	CVE-2025-68973	GnuPG	Локальный	ACE	2025-12-29	✗
37	Критическая	CVE-2025-59719	Fortinet products	Сетевой	SB	2025-12-10	✓
38	Критическая	CVE-2025-59718	Fortinet products	Сетевой	SB	2025-12-10	✓
39	Критическая	CVE-2025-20337	Cisco Identity Services Engine	Сетевой	ACE	2025-06-25	✓
40	Критическая	CVE-2025-20282	Cisco Identity Services Engine	Сетевой	ACE	2025-06-25	✓
41	Критическая	CVE-2025-20281	Cisco Identity Services Engine	Сетевой	ACE	2025-06-25	✓

1

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2026-0881

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Mozilla Thunderbird:
141.0 - 146.0

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-04/

2

Краткое описание: Отказ в обслуживании в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2026-0884

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Thunderbird:
141.0 - 146.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-04/

3

Краткое описание: Отказ в обслуживании в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2026-0889

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Mozilla Thunderbird:
141.0 - 146.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Отказ в обслуживании

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

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

Оценка CVSSv4: 0.5 AV:N/AC:H/AT:N/PR:N/UI:A/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:U/U:Clear

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-04/

4

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird

Идентификатор уязвимости: CVE-2026-0892

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

Уязвимый продукт: Mozilla Thunderbird:
141.0 - 146.0

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-04/

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-0891

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

Уязвимый продукт: Mozilla Thunderbird:
141.0 - 146.0
Mozilla Thunderbird:
128.0 - 140.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-04/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-05/

6

Краткое описание: Отказ в обслуживании в Mozilla Thunderbird ESR

Идентификатор уязвимости: CVE-2026-0884

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Thunderbird:
128.0 - 140.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-05/

7

Краткое описание: Получение конфиденциальной информации в Mozilla Thunderbird ESR

Идентификатор уязвимости: CVE-2025-14327

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

Уязвимый продукт: Mozilla Thunderbird:
128.0 - 140.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Получение конфиденциальной информации

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-05/

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-0882

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Thunderbird:
141.0 - 146.0
Mozilla Thunderbird:
128.0 - 140.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

Последствия эксплуатации: Выполнение произвольного кода

8 **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: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-04/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-05/

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-0880

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

Уязвимый продукт: Mozilla Thunderbird:
141.0 - 146.0
Mozilla Thunderbird:
128.0 - 140.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 6.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-04/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-05/

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-0879

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

Уязвимый продукт: Mozilla Thunderbird:
141.0 - 146.0
Mozilla Thunderbird:
128.0 - 140.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-04/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-05/

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-0878

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

Уязвимый продукт: Mozilla Thunderbird:
141.0 - 146.0
Mozilla Thunderbird:
128.0 - 140.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 8.0 AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-04/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-05/

Краткое описание: Выполнение произвольного кода в Mozilla Thunderbird и Thunderbird ESR

Идентификатор уязвимости: CVE-2026-0877

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: Mozilla Thunderbird:
141.0 - 146.0
Mozilla Thunderbird:
128.0 - 140.6.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

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

Оценка CVSSv4: 6.0 AV:N/AC:L/AT:N/PR:N/UI:A/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:U/U:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2026-04/
- https://www.mozilla.org/en-US/security/advisories/mfsa2026-05/

13

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

Идентификатор уязвимости: CVE-2026-21287

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Substance 3D Stager:
2.0.0 - 3.1.5

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: 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: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_stager/apsb26-09.html

14

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

Идентификатор уязвимости: CVE-2026-21305

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Substance 3D Painter: 10.0.0 - 11.0.3

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: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d_painter/apsb26-10.html

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

Идентификатор уязвимости: CVE-2026-21306

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Adobe Substance 3D Sampler:
4.0.0 - 5.1.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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: 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: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://helpx.adobe.com/security/products/substance3d-sampler/apsb26-11.html

16

Краткое описание: Выполнение произвольного кода в Adobe Bridge

Идентификатор уязвимости: CVE-2026-21283

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

Уязвимый продукт: Adobe Bridge:
14.0.0 - 16.0

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: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://helpx.adobe.com/security/products/bridge/apsb26-07.html

17

Краткое описание: Выполнение произвольного кода в Adobe Illustrator

Идентификатор уязвимости: CVE-2026-21280

Идентификатор программной ошибки: CWE-427 Неконтролируемый элемент пути поиска

Уязвимый продукт: Adobe Illustrator:
22.0 - 30.0

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: 8.6 AV:L/AC:L/PR:N/UI:R/S:C/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: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://helpx.adobe.com/security/products/illustrator/apsb26-03.html

18

Краткое описание: Выполнение произвольного кода в Adobe InCopy

Идентификатор уязвимости: CVE-2026-21281

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

Уязвимый продукт: InCopy:
18.0 - 21.0

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: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://helpx.adobe.com/security/products/incopy/apsb26-04.html

19

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-21304

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

Уязвимый продукт: Adobe InDesign:
18.0 - 21.0

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: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-02.html

20

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-21277

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

Уязвимый продукт: Adobe InDesign:
18.0 - 21.0

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: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-02.html

21

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-21276

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Adobe InDesign:
18.0 - 21.0

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: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-02.html

22

Краткое описание: Выполнение произвольного кода в Adobe InDesign

Идентификатор уязвимости: CVE-2026-21275

Идентификатор программной ошибки: CWE-824 Обращение к неинициализированному указателю

Уязвимый продукт: Adobe InDesign:
18.0 - 21.0

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: 2026-01-15 / 2026-01-15

Ссылки на источник:

- https://helpx.adobe.com/security/products/indesign/apsb26-02.html

Краткое описание: Получение конфиденциальной информации в n8n

Идентификатор уязвимости: CVE-2026-21858
BDU:2026-00126

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: n8n:
1.65.0 - 1.121.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Получение конфиденциальной информации

23

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:N

Оценка CVSSv4: Не определено

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-07 / 2026-01-12

Ссылки на источник:

- https://nvd.nist.gov/vuln/detail/CVE-2026-21858
- https://bdu.fstec.ru/vul/2026-00126

24

Краткое описание: Получение конфиденциальной информации в n8n

Идентификатор уязвимости: CVE-2025-68613

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

Уязвимый продукт: n8n:
0.211.0 - 1.121.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Отправка 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: 9.9 AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Оценка CVSSv4: 8.6 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N/E:A/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-23 / 2025-12-23

Ссылки на источник:

- https://github.com/n8n-io/n8n/security/advisories/GHSA-v98v-ff95-f3cp

Краткое описание: Выполнение произвольного кода в n8n

Идентификатор уязвимости: CVE-2025-68668

Идентификатор программной ошибки: CWE-693 Некорректное использование защитных механизмов

Уязвимый продукт: n8n:
1.0.0 - 1.123.9

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход ограничений безопасности

Последствия эксплуатации: Выполнение произвольного кода

25

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:L

Оценка CVSSv4: 6.3 AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-07 / 2026-01-07

Ссылки на источник:

- https://github.com/advisories/GHSA-62r4-hw23-cc8v

26

Краткое описание: Выполнение произвольного кода в Cisco Secure Email Gateway And Cisco Secure Email and Web Manager

Идентификатор уязвимости: CVE-2025-20393
BDU:2025-16120

Идентификатор программной ошибки: CWE-20 Некорректная проверка входных данных

Уязвимый продукт: Secure Email Gateway:
все версии
Cisco Secure Email and Web Manager:
все версии

Категория уязвимого продукта: Телекоммуникационное оборудование

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 9.3 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-17 / 2025-12-17

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCws36549
- https://bdu.fstec.ru/vul/2025-16120

27

Краткое описание: Выполнение произвольного кода в WatchGuard Firebox iked

Идентификатор уязвимости: CVE-2025-14733
BDU:2025-16142

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Fireware OS:
11.10.2 - 2025.1.3

Категория уязвимого продукта: Средства защиты информации

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

Оценка CVSSv4: 9.3 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-19 / 2025-12-19

Ссылки на источник:

- https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00027
- https://bdu.fstec.ru/vul/2025-16142

Краткое описание: Выполнение произвольного кода в GIMP

Идентификатор уязвимости: CVE-2025-15059

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.

28

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: 2026-01-12 / 2026-01-12

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1196/
- https://gitlab.gnome.org/GNOME/gimp/-/commit/03575ac8cbb0ef3103b0a15d6598475088dcc15e

Краткое описание: Получение конфиденциальной информации в AzeoTech DAQFactory

Идентификатор уязвимости: CVE-2025-66589

Идентификатор программной ошибки: CWE-125 Чтение за пределами буфера

Уязвимый продукт: DAQFactory:
20.7 2555 and previous versions

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

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.

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-09 / 2026-01-09

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1156/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-345-03
- https://www.zerodayinitiative.com/advisories/ZDI-25-1157/
- https://www.zerodayinitiative.com/advisories/ZDI-25-1158/
- https://www.zerodayinitiative.com/advisories/ZDI-25-1159/
- https://www.zerodayinitiative.com/advisories/ZDI-25-1160/
- https://www.zerodayinitiative.com/advisories/ZDI-25-1161/

Краткое описание: Выполнение произвольного кода в AzeoTech DAQFactory

Идентификатор уязвимости: CVE-2025-66585

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: DAQFactory:
20.7 2555 and previous versions

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

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.

30

Оценка CVSSv3: 7.8 AV:L/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: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-01-09 / 2026-01-09

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1128/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-345-03

31

Краткое описание: Выполнение произвольного кода в AzeoTech DAQFactory

Идентификатор уязвимости: CVE-2025-66586

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

Уязвимый продукт: DAQFactory:
20.7 2555 and previous versions

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

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

Оценка CVSSv4: 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: Локальный

Взаимодействие с пользователем: Требуется

Дата выявления / Дата обновления: 2026-01-09 / 2026-01-09

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1131/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-345-03
- https://www.zerodayinitiative.com/advisories/ZDI-25-1132/
- https://www.zerodayinitiative.com/advisories/ZDI-25-1133/
- https://www.zerodayinitiative.com/advisories/ZDI-25-1134/

Краткое описание: Выполнение произвольного кода в AzeoTech DAQFactory

Идентификатор уязвимости: CVE-2025-66590

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: DAQFactory:
20.7 2555 and previous versions

Категория уязвимого продукта: Промышленное программно-аппаратное оборудование

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

32

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2026-01-09 / 2026-01-09

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1162/
- https://www.zerodayinitiative.com/advisories/ZDI-25-1129/
- https://www.zerodayinitiative.com/advisories/ZDI-25-1130/
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-345-03

Краткое описание: Выполнение произвольного кода в TOTOLINK EX200

Идентификатор уязвимости: CVE-2025-65606

Идентификатор программной ошибки: CWE-388 Уязвимости, связанные с обработкой ошибок

Уязвимый продукт: EX200:
все версии

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: Не определено

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: Не определено

Взаимодействие с пользователем: Не определено

Дата выявления / Дата обновления: 2026-01-08 / 2026-01-08

Ссылки на источник:

- https://www.kb.cert.org/vuls/id/295169

Краткое описание: Получение конфиденциальной информации в GNU wget

Идентификатор уязвимости: CVE-2025-69194

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

Уязвимый продукт: wget:
2.0.0 - 2.2.0

Категория уязвимого продукта: Серверное программное обеспечение и его компоненты

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

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.

34

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: 2026-01-07 / 2026-01-07

Ссылки на источник:

- https://bugzilla.redhat.com/show_bug.cgi?id=2425773
- https://gitlab.com/gnuwget/wget2/-/commit/485c6aa5ba38cb369c6eb8564ea97cddc854049e

Краткое описание: Обход безопасности в Google Chrome и Microsoft Edge

Идентификатор уязвимости: CVE-2026-0628

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

Уязвимый продукт: Google Chrome:
100.0.4896.60 - 143.0.7499.170
Microsoft Edge:
100.0.1185.29 - 143.0.3650.96

Категория уязвимого продукта: Прикладное программное обеспечение

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

Последствия эксплуатации: Обход безопасности

35

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

Оценка CVSSv3: 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: 2026-01-06 / 2026-01-06

Ссылки на источник:

- https://chromereleases.googleblog.com/2026/01/stable-channel-update-for-desktop.html
- https://crbug.com/463155954
- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2026-0628

36

Краткое описание: Выполнение произвольного кода в GnuPG

Идентификатор уязвимости: CVE-2025-68973

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: GnuPG:
все версии

Категория уязвимого продукта: Средства защиты информации

Способ эксплуатации: Отправка специально сформированных данных.

Последствия эксплуатации: Выполнение произвольного кода

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

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-29 / 2025-12-29

Ссылки на источник:

- https://seclists.org/oss-sec/2025/q4/311
- https://gpg.fail/memcpy

Краткое описание: Обход безопасности в Fortinet products

Идентификатор уязвимости: CVE-2025-59719

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: FortiOS:
7.0.0 - 7.6.3
FortiProxy:
7.0.0 - 7.6.3
FortiSwitch Manager:
7.0.0 - 7.2.6
FortiWeb:
7.4.0 - 8.0.0

Категория уязвимого продукта: Телекоммуникационное оборудование

37 **Способ эксплуатации:** Отправка специально сформированных данных.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: 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: 2025-12-10 / 2025-12-10

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-25-647

Краткое описание: Обход безопасности в Fortinet products

Идентификатор уязвимости: CVE-2025-59718

Идентификатор программной ошибки: CWE-347 Некорректная проверка криптографической подписи

Уязвимый продукт: FortiOS:
7.0.0 - 7.6.3
FortiProxy:
7.0.0 - 7.6.3
FortiSwitch Manager:
7.0.0 - 7.2.6
FortiWeb:
7.4.0 - 8.0.0

Категория уязвимого продукта: Телекоммуникационное оборудование

38 **Способ эксплуатации:** Отправка специально сформированных данных.

Последствия эксплуатации: Обход безопасности

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

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

Оценка CVSSv4: 9.2 AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.fortiguard.com/psirt/FG-IR-25-647

39

Краткое описание: Выполнение произвольного кода в Cisco Identity Services Engine

Идентификатор уязвимости: CVE-2025-20337

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

Уязвимый продукт: Cisco Identity Services Engine (ISE):
3.3 - 3.4P1

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Оценка CVSSv4: 9.3 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-06-25 / 2025-06-25

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwp02814

Краткое описание: Выполнение произвольного кода в Cisco Identity Services Engine

Идентификатор уязвимости: CVE-2025-20282

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

Уязвимый продукт: Cisco Identity Services Engine (ISE):
3.4 - 3.4P1

Категория уязвимого продукта: Телекоммуникационное оборудование

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.

40

Оценка CVSSv3: 10.0 AV:N/AC:L/PR:N/UI:N/S:C/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:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-06-25 / 2025-06-25

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwp02821

41

Краткое описание: Выполнение произвольного кода в Cisco Identity Services Engine

Идентификатор уязвимости: CVE-2025-20281

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

Уязвимый продукт: Cisco Identity Services Engine (ISE):
3.3 - 3.4P1

Категория уязвимого продукта: Телекоммуникационное оборудование

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

Оценка CVSSv4: 9.3 AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:A/U:Red

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-06-25 / 2025-06-25

Ссылки на источник:

- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-unauth-rce-ZAd2GnJ6
- https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwo99449