НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

Бюллетень об уязвимостях программного обеспечения

VULN.2025-12-22.1 | 22 декабря 2025 года

TLP: WHITE

Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Высокая	CVE-2025-66499	Foxit PDF Reader and PDF Editor for Windows	Локальный	ACE	2025-12-19	✓
2	Высокая	CVE-2025-13941	Foxit PDF Reader and PDF Editor for Windows	Локальный	ACE	2025-12-19	✓
3	Высокая	CVE-2025-66495	Foxit PDF Reader and PDF Editor for Windows	Локальный	ACE	2025-12-19	✓
4	Высокая	CVE-2025-66494	Foxit PDF Reader and PDF Editor for Windows	Локальный	ACE	2025-12-19	✓
5	Высокая	CVE-2025-66493	Foxit PDF Reader and PDF Editor for Windows	Локальный	ACE	2025-12-19	✓
6	Высокая	CVE-2025-14765	Microsoft Edge	Сетевой	ACE	2025-12-19	✓
7	Высокая	CVE-2025-14766	Microsoft Edge	Сетевой	ACE	2025-12-19	✓
8	Высокая	CVE-2025-14861	Mozilla Firefox	Сетевой	ACE	2025-12-18	✓
9	Критическая	CVE-2025-14860	Mozilla Firefox	Сетевой	ACE	2025-12-18	✓
10	Высокая	CVE-2025-14424	Gimp	Локальный	ACE	2025-12-18	✓
11	Высокая	CVE-2025-14425	Gimp	Локальный	ACE	2025-12-18	✓
12	Высокая	CVE-2025-14423	Gimp	Локальный	ACE	2025-12-18	✓

13	Высокая	CVE-2025-14422	Gimp	Локальный	ACE	2025-12-18	✓
14	Высокая	CVE-2024-55549	Tenable Nessus	Локальный	ACE	2025-12-15	✓
15	Высокая	CVE-2025-7425	Tenable Nessus	Локальный	ACE	2025-12-15	✓
16	Критическая	CVE-2025-49796	Tenable Nessus	Сетевой	DoS	2025-12-15	✓
17	Высокая	CVE-2025-6021	Tenable Nessus	Сетевой	ACE	2025-12-15	✓
18	Критическая	CVE-2025-49794	Tenable Nessus	Сетевой	DoS	2025-12-15	✓
19	Высокая	CVE-2025-59375	Tenable Nessus	Сетевой	DoS	2025-12-15	✓
20	Высокая	CVE-2024-8176	Tenable Nessus	Сетевой	ACE	2025-12-15	✓

1

Краткое описание: Выполнение произвольного кода в Foxit PDF Reader and PDF Editor for Windows

Идентификатор уязвимости: CVE-2025-66499

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

Уязвимый продукт: Foxit PDF Reader for Windows:
2023.2.0.21408 - 2025.2.1.33197
Foxit PDF Editor (formerly Foxit PhantomPDF):
13.0.0.21632 - 2025.2.1.33197

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного PDF-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: 2025-12-19 / 2025-12-19

Ссылки на источник:

- https://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+2025.3+and+Foxit+PDF+Editor+2025.3%2F14.0.2%2F13.2.22025-12-19+00%3A00%3A00

2

Краткое описание: Выполнение произвольного кода в Foxit PDF Reader and PDF Editor for Windows

Идентификатор уязвимости: CVE-2025-13941

Идентификатор программной ошибки: CWE-732 Некорректные разрешения для критически важных ресурсов

Уязвимый продукт: Foxit PDF Reader for Windows:
2023.2.0.21408 - 2025.2.1.33197
Foxit PDF Editor (formerly Foxit PhantomPDF):
13.0.0.21632 - 2025.2.1.33197

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

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

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

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

Ссылки на источник:

- https://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+2025.3+and+Foxit+PDF+Editor+2025.3%2F14.0.2%2F13.2.22025-12-19+00%3A00%3A00

3

Краткое описание: Выполнение произвольного кода в Foxit PDF Reader and PDF Editor for Windows

Идентификатор уязвимости: CVE-2025-66495

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Foxit PDF Reader for Windows:
2023.2.0.21408 - 2025.2.1.33197
Foxit PDF Editor (formerly Foxit PhantomPDF):
13.0.0.21632 - 2025.2.1.33197

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: 2025-12-19 / 2025-12-19

Ссылки на источник:

- https://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+2025.3+and+Foxit+PDF+Editor+2025.3%2F14.0.2%2F13.2.22025-12-19+00%3A00%3A00

4

Краткое описание: Выполнение произвольного кода в Foxit PDF Reader and PDF Editor for Windows

Идентификатор уязвимости: CVE-2025-66494

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Foxit PDF Reader for Windows:
2023.2.0.21408 - 2025.2.1.33197
Foxit PDF Editor (formerly Foxit PhantomPDF):
13.0.0.21632 - 2025.2.1.33197

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: 2025-12-19 / 2025-12-19

Ссылки на источник:

- https://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+2025.3+and+Foxit+PDF+Editor+2025.3%2F14.0.2%2F13.2.22025-12-19+00%3A00%3A00

5

Краткое описание: Выполнение произвольного кода в Foxit PDF Reader and PDF Editor for Windows

Идентификатор уязвимости: CVE-2025-66493

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Foxit PDF Reader for Windows:
2023.2.0.21408 - 2025.2.1.33197
Foxit PDF Editor (formerly Foxit PhantomPDF):
13.0.0.21632 - 2025.2.1.33197

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: 2025-12-19 / 2025-12-19

Ссылки на источник:

- https://www.foxitsoftware.com/support/security-bulletins.html?Security+updates+available+in+Foxit+PDF+Reader+2025.3+and+Foxit+PDF+Editor+2025.3%2F14.0.2%2F13.2.22025-12-19+00%3A00%3A00

6

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2025-14765

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Microsoft Edge:
100.0.1185.29 - 143.0.3650.80

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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: 2025-12-19 / 2025-12-19

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-14765

7

Краткое описание: Выполнение произвольного кода в Microsoft Edge

Идентификатор уязвимости: CVE-2025-14766

Идентификатор программной ошибки: CWE-787 Запись за границами буфера

Уязвимый продукт: Microsoft Edge:
100.0.1185.29 - 143.0.3650.80

Категория уязвимого продукта: Операционные системы Microsoft и их компоненты

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:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Требуется

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

Ссылки на источник:

- https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2025-14766

8

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-14861

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

Уязвимый продукт: Mozilla Firefox:
140.0 - 146.0
Firefox for Android:
140.0 - 146.0

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: 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: 2025-12-18 / 2025-12-18

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-98/
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1996570
- https://bugzilla.mozilla.org/buglist.cgi?bug_id=1999700

Краткое описание: Выполнение произвольного кода в Mozilla Firefox

Идентификатор уязвимости: CVE-2025-14860

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Mozilla Firefox:
140.0 - 146.0
Firefox for Android:
140.0 - 146.0

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-18 / 2025-12-18

Ссылки на источник:

- https://www.mozilla.org/en-US/security/advisories/mfsa2025-98/
- https://bugzilla.mozilla.org/show_bug.cgi?id=2000597

Краткое описание: Выполнение произвольного кода в Gimp

Идентификатор уязвимости: CVE-2025-14424

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Gimp:
2.10.0 - 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: 2025-12-18 / 2025-12-18

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1138/
- https://gitlab.gnome.org/GNOME/gimp/-/commit/5cc55d078b7fba995cef77d195fac325ee288ddd

Краткое описание: Выполнение произвольного кода в Gimp

Идентификатор уязвимости: CVE-2025-14425

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

Уязвимый продукт: Gimp:
2.10.0 - 3.1.4

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Открытие пользователем специально созданного вредоносного файла.

Последствия эксплуатации: Выполнение произвольного кода

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

Оценка CVSSv3: 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: 2025-12-18 / 2025-12-18

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1139/
- https://gitlab.gnome.org/GNOME/gimp/-/commit/cd1c88a0364ad1444c06536731972a99bd8643fd

Краткое описание: Выполнение произвольного кода в Gimp

Идентификатор уязвимости: CVE-2025-14423

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.

12

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: 2025-12-18 / 2025-12-18

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1137/
- https://gitlab.gnome.org/GNOME/gimp/-/commit/481cdbbb97746be1145ec3a633c567a68633c521

Краткое описание: Выполнение произвольного кода в Gimp

Идентификатор уязвимости: CVE-2025-14422

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

Уязвимый продукт: Gimp:
2.5.3 - 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.

13

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: 2025-12-18 / 2025-12-18

Ссылки на источник:

- https://www.zerodayinitiative.com/advisories/ZDI-25-1136/
- https://gitlab.gnome.org/GNOME/gimp/-/commit/4ff2d773d58064e6130495de498e440f4a6d5edb

14

Краткое описание: Выполнение произвольного кода в Tenable Nessus

Идентификатор уязвимости: CVE-2024-55549

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Tenable Nessus:
10.0.0 - 10.11.0

Категория уязвимого продукта: Прикладное программное обеспечение

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: 7.8 AV:L/AC:H/PR:N/UI:N/S:C/C:N/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: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-15 / 2025-12-15

Ссылки на источник:

- https://www.tenable.com/security/tns-2025-24

Краткое описание: Выполнение произвольного кода в Tenable Nessus

Идентификатор уязвимости: CVE-2025-7425

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Tenable Nessus:
10.0.0 - 10.11.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Использование памяти после ее освобождения

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:H/PR:N/UI:N/S:C/C:N/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:Amber

Вектор атаки: Локальный

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-15 / 2025-12-15

Ссылки на источник:

- https://www.tenable.com/security/tns-2025-24

16

Краткое описание: Отказ в обслуживании в Tenable Nessus

Идентификатор уязвимости: CVE-2025-49796

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

Уязвимый продукт: Tenable Nessus:
10.0.0 - 10.11.0

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

Оценка CVSSv4: 2.7 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-15 / 2025-12-15

Ссылки на источник:

- https://www.tenable.com/security/tns-2025-24

17

Краткое описание: Выполнение произвольного кода в Tenable Nessus

Идентификатор уязвимости: CVE-2025-6021

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

Уязвимый продукт: Tenable Nessus:
10.0.0 - 10.11.0

Категория уязвимого продукта: Прикладное программное обеспечение

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: 7.5 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:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-15 / 2025-12-15

Ссылки на источник:

- https://www.tenable.com/security/tns-2025-24

18

Краткое описание: Отказ в обслуживании в Tenable Nessus

Идентификатор уязвимости: CVE-2025-49794

Идентификатор программной ошибки: CWE-416 Использование после освобождения

Уязвимый продукт: Tenable Nessus:
10.0.0 - 10.11.0

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

Оценка CVSSv4: 2.7 AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N/E:U/U:Green

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-15 / 2025-12-15

Ссылки на источник:

- https://www.tenable.com/security/tns-2025-24

19

Краткое описание: Отказ в обслуживании в Tenable Nessus

Идентификатор уязвимости: CVE-2025-59375

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

Уязвимый продукт: Tenable Nessus:
10.0.0 - 10.11.0

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Исчерпание ресурсов.

Последствия эксплуатации: Отказ в обслуживании

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

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

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-15 / 2025-12-15

Ссылки на источник:

- https://www.tenable.com/security/tns-2025-24

20

Краткое описание: Выполнение произвольного кода в Tenable Nessus

Идентификатор уязвимости: CVE-2024-8176

Идентификатор программной ошибки: CWE-121 Переполнение буфера в стеке

Уязвимый продукт: Tenable Nessus:
10.0.0 - 10.11.0

Категория уязвимого продукта: Прикладное программное обеспечение

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: 7.5 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:Amber

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2025-12-15 / 2025-12-15

Ссылки на источник:

- https://www.tenable.com/security/tns-2025-24