

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: [cert.gov.ru](https://cert.gov.ru)

E-mail: [threats@cert.gov.ru](mailto:threats@cert.gov.ru)

## Бюллетень об уязвимостях программного обеспечения

VULN.2024-11-06.1 | 6 ноября 2024 года

TLP: WHITE



## Перечень уязвимостей

№ п/п	Опасность	Идентификатор	Уязвимый продукт	Вектор атаки	Последствия	Дата выявления	Наличие обновления
1	Критическая	CVE-2024-9931	Wux Blog Editor plugin for WordPress	Сетевой	SB	2024-11-04	✗
2	Критическая	CVE-2024-9488	Comments – wpDiscuz plugin for WordPress	Сетевой	SB	2024-11-04	✓
3	Критическая	CVE-2024-9932	Wux Blog Editor plugin for WordPress	Сетевой	WLF	2024-11-04	✗
4	Критическая	CVE-2024-9501	Wp Social Login and Register Social Counter plugin for WordPress	Сетевой	SB	2024-11-04	✓
5	Высокая	CVE-2024-10467	Mozilla	Сетевой	ACE	2024-10-29	✓
6	Высокая	CVE-2024-10466	Mozilla	Сетевой	DoS	2024-10-29	✓
7	Высокая	CVE-2024-10459	Mozilla	Сетевой	ACE	2024-10-29	✓
8	Высокая	CVE-2024-10458	Mozilla	Сетевой	SB	2024-10-29	✓
9	Критическая	CVE-2024-9369	Google ChromeOS	Сетевой	ACE	2024-10-29	✓
10	Высокая	CVE-2024-7971	Google ChromeOS	Сетевой	ACE	2024-10-29	✓
11	Высокая	CVE-2024-10488	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-10-30	✓
12	Высокая	CVE-2024-10487	Google Chrome и Microsoft Edge	Сетевой	ACE	2024-10-30	✓
13	Высокая	CVE-2024-9997	Autodesk AutoCAD и AutoCAD-based products	Локальный	ACE	2024-10-30	✓

14	Высокая	CVE-2024-9996	Autodesk AutoCAD и AutoCAD-based products	Локальный	ACE	2024-10-30	✓
15	Высокая	CVE-2024-9489	Autodesk AutoCAD и AutoCAD-based products	Локальный	ACE	2024-10-30	✓
16	Высокая	CVE-2024-8896	Autodesk AutoCAD и AutoCAD-based products	Локальный	SB	2024-10-30	✓
17	Высокая	CVE-2024-7992	Autodesk AutoCAD и AutoCAD-based products	Локальный	ACE	2024-10-30	✓
18	Высокая	CVE-2024-7991	Autodesk AutoCAD и AutoCAD-based products	Локальный	ACE	2024-10-30	✓
19	Высокая	CVE-2024-8587	Autodesk AutoCAD and AutoCAD-based products	Локальный	ACE	2024-10-30	✓
20	Высокая	CVE-2024-8588	Autodesk AutoCAD and AutoCAD-based products	Локальный	OSI	2024-10-30	✓
21	Высокая	CVE-2024-8589	Autodesk AutoCAD and AutoCAD-based products	Локальный	OSI	2024-10-30	✓
22	Высокая	CVE-2024-8590	Autodesk AutoCAD and AutoCAD-based products	Локальный	ACE	2024-10-30	✓
23	Высокая	CVE-2024-8591	Autodesk AutoCAD and AutoCAD-based products	Локальный	ACE	2024-10-30	✓
24	Высокая	CVE-2024-8593	Autodesk AutoCAD and AutoCAD-based products	Локальный	ACE	2024-10-30	✓
25	Высокая	CVE-2024-8594	Autodesk AutoCAD and AutoCAD-based products	Локальный	ACE	2024-10-30	✓

26	Высокая	CVE-2024-8595	Autodesk AutoCAD and AutoCAD-based products	Локальный	ACE	2024-10-30	✓
27	Высокая	CVE-2024-8597	Autodesk AutoCAD and AutoCAD-based products	Локальный	ACE	2024-10-30	✓
28	Высокая	CVE-2024-8598	Autodesk AutoCAD and AutoCAD-based products	Локальный	ACE	2024-10-30	✓
29	Высокая	CVE-2024-8599	Autodesk AutoCAD and AutoCAD-based products	Локальный	ACE	2024-10-30	✓
30	Высокая	CVE-2024-8600	Autodesk AutoCAD and AutoCAD-based products	Локальный	ACE	2024-10-30	✓
31	Высокая	CVE-2024-9826	Autodesk AutoCAD and AutoCAD-based products	Локальный	ACE	2024-10-30	✓
32	Высокая	CVE-2024-9827	Autodesk AutoCAD and AutoCAD-based products	Локальный	OSI	2024-10-30	✓
33	Высокая	CVE-2024-8596	Autodesk AutoCAD и AutoCAD-based products	Локальный	ACE	2024-10-30	✓
34	Высокая	CVE-2024-38415	Qualcomm chipsets	Локальный	ACE	2024-11-04	✓
35	Высокая	CVE-2024-38419	Qualcomm chipsets	Локальный	ACE	2024-11-04	✓
36	Высокая	CVE-2024-38422	Qualcomm chipsets	Локальный	ACE	2024-11-04	✓
37	Высокая	CVE-2024-38421	Qualcomm chipsets	Локальный	ACE	2024-11-04	✓
38	Высокая	CVE-2024-38423	Qualcomm chipsets	Локальный	ACE	2024-11-04	✓

39	Высокая	CVE-2024-23385	Qualcomm chipsets	Сетевой	DoS	2024-11-04	✓
40	Высокая	CVE-2024-38408	Qualcomm chipsets	Сетевой	ACE	2024-11-04	✓
41	Высокая	CVE-2024-38403	Qualcomm chipsets	Сетевой	DoS	2024-11-04	✓
42	Высокая	CVE-2024-38406	Qualcomm chipsets	Локальный	ACE	2024-11-04	✓
43	Высокая	CVE-2024-38407	Qualcomm chipsets	Локальный	ACE	2024-11-04	✓
44	Высокая	CVE-2024-38409	Qualcomm chipsets	Локальный	ACE	2024-11-04	✓
45	Высокая	CVE-2024-38410	Qualcomm chipsets	Локальный	ACE	2024-11-04	✓
46	Высокая	CVE-2024-38424	Qualcomm chipsets	Локальный	ACE	2024-11-04	✓
47	Высокая	CVE-2024-33068	Qualcomm chipsets	Сетевой	DoS	2024-11-04	✓
48	Высокая	CVE-2024-38405	Qualcomm chipsets	Сетевой	DoS	2024-11-04	✓
49	Высокая	CVE-2024-47904	Siemens InterMesh Subscriber Devices	Локальный	ACE	2024-10-31	✓
50	Критическая	CVE-2024-47901	Siemens InterMesh Subscriber Devices	Сетевой	ACE	2024-10-31	✓

**Краткое описание:** Обход безопасности в Wux Blog Editor plugin for WordPress

**Идентификатор уязвимости:** CVE-2024-9931

**Идентификатор программной ошибки:** CWE-287 Некорректная аутентификация

**Уязвимый продукт:** Wux Blog Editor: с версии 1.0.0 по 3.0.0

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Обход процесса аутентификации

**Последствия эксплуатации:** Обход безопасности

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://www.wordfence.com/threat-intel/vulnerabilities/id/494ef738-c900-4d00-8739-3b261586d4ff?source=cve>
- [http://plugins.trac.wordpress.org/browser/wux-blog-editor/tags/3.0.0/External\\_Post\\_Editor.php#L675](http://plugins.trac.wordpress.org/browser/wux-blog-editor/tags/3.0.0/External_Post_Editor.php#L675)

Краткое описание: Обход безопасности в Comments – wpDiscuz plugin for WordPress

Идентификатор уязвимости: CVE-2024-9488

Идентификатор программной ошибки: CWE-287 Некорректная аутентификация

Уязвимый продукт: Comments – wpDiscuz: с версии 7.6.0 по 7.6.24

Категория уязвимого продукта: Прикладное программное обеспечение

Способ эксплуатации: Обход процесса аутентификации

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

Вектор атаки: Сетевой

Взаимодействие с пользователем: Отсутствует

Дата выявления / Дата обновления: 2024-11-04 / 2024-11-04

Ссылки на источник:

- <http://www.wordfence.com/threat-intel/vulnerabilities/id/b71706a7-e101-4d50-a2da-1aeeaf07cf4b?source=cve>
- <http://plugins.trac.wordpress.org/browser/wpdiscuz/trunk/forms/wpFormAttr/Login/SocialLogin.php>
- <http://plugins.trac.wordpress.org/changeset/3164486/>

**Краткое описание:** Запись локальных файлов в Wux Blog Editor plugin for WordPress

**Идентификатор уязвимости:** CVE-2024-9932

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

**Уязвимый продукт:** Wux Blog Editor: с версии 1.0.0 по 3.0.0

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Отправка специально созданного вредоносного файла.

**Последствия эксплуатации:** Запись локальных файлов

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://www.wordfence.com/threat-intel/vulnerabilities/id/c2c0ab2d-1ba9-4a0a-b1fa-bacebe1034eb?source=cve>
- [http://plugins.trac.wordpress.org/browser/wux-blog-editor/tags/3.0.0/External\\_Post\\_Editor.php#L675](http://plugins.trac.wordpress.org/browser/wux-blog-editor/tags/3.0.0/External_Post_Editor.php#L675)

**Краткое описание:** Обход безопасности в Wp Social Login and Register Social Counter plugin for WordPress

**Идентификатор уязвимости:** CVE-2024-9501

**Идентификатор программной ошибки:** CWE-287 Некорректная аутентификация

**Уязвимый продукт:** Wp Social: с версии 3.0.0 по 3.0.7

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Обход процесса аутентификации

**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:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://www.wordfence.com/threat-intel/vulnerabilities/id/a4294f5f-d989-4b97-88ee-4e94f4f7845a?source=cve>
- <http://plugins.trac.wordpress.org/browser/wp-social/tags/3.0.6/inc/admin-create-user.php#L205>
- <http://plugins.trac.wordpress.org/changeset/3173675/>

**Краткое описание:** Выполнение произвольного кода в Mozilla

**Идентификатор уязвимости:** CVE-2024-10467

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

**Уязвимый продукт:** Mozilla:

Mozilla Firefox: с версии 100.0 по 131.0.3

Firefox ESR: с версии 102.0 по 128.3.1

Firefox for Android: с версии 100.1.0 по 131.0.2

Mozilla Thunderbird: с версии 125.0 по 129.0

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

5 **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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-29 / 2024-10-29

**Ссылки на источник:**

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-55/>
- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-56/>

**Краткое описание:** Отказ в обслуживании в Mozilla

**Идентификатор уязвимости:** CVE-2024-10466

**Идентификатор программной ошибки:** CWE-399 Уязвимости, связанные с управлением ресурсами

**Уязвимый продукт:** Mozilla:

Mozilla Firefox: с версии 100.0 по 131.0.3

Firefox ESR: с версии 102.0 по 128.3.1

Firefox for Android: с версии 100.1.0 по 131.0.2

Mozilla Thunderbird: с версии 125.0 по 129.0

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

6

**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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-29 / 2024-10-29

**Ссылки на источник:**

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-55/>
- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-56/>

**Краткое описание:** Выполнение произвольного кода в Mozilla

**Идентификатор уязвимости:** CVE-2024-10459

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Mozilla:

Mozilla Firefox: с версии 100.0 по 131.0.3

Firefox ESR: с версии 102.0 по 128.3.1

Firefox for Android: с версии 100.1.0 по 131.0.2

Mozilla Thunderbird: с версии 125.0 по 129.0

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-29 / 2024-10-29

**Ссылки на источник:**

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-55/>
- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-56/>
- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-57/>

**Краткое описание:** Обход безопасности в Mozilla

**Идентификатор уязвимости:** CVE-2024-10458

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

**Уязвимый продукт:** Mozilla:

Mozilla Firefox: с версии 100.0 по 131.0.3

Firefox ESR: с версии 102.0 по 128.3.1

Firefox for Android: с версии 100.1.0 по 131.0.2

Mozilla Thunderbird: с версии 125.0 по 129.0

**Категория уязвимого продукта:** Прикладное программное обеспечение

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-29 / 2024-10-29

**Ссылки на источник:**

- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-55/>
- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-56/>
- <http://www.mozilla.org/en-US/security/advisories/mfsa2024-57/>

**Краткое описание:** Выполнение произвольного кода в Google ChromeOS

**Идентификатор уязвимости:** CVE-2024-9369  
BDU:2024-08729

**Идентификатор программной ошибки:** CWE-20 Некорректная проверка входных данных

**Уязвимый продукт:** Chrome OS: до версии 126.0.6478.256

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

**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:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-29 / 2024-10-29

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/10/long-term-support-channel-update-for\\_29.html](http://chromereleases.googleblog.com/2024/10/long-term-support-channel-update-for_29.html)
- <https://bdu.fstec.ru/vul/2024-08729>

**Краткое описание:** Выполнение произвольного кода в Google ChromeOS

**Идентификатор уязвимости:** CVE-2024-7971  
BDU:2024-06562

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

**Уязвимый продукт:** Chrome OS: до версии 126.0.6478.256

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

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

**Последствия эксплуатации:** Выполнение произвольного кода

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

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-29 / 2024-10-29

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/10/long-term-support-channel-update-for\\_29.html](http://chromereleases.googleblog.com/2024/10/long-term-support-channel-update-for_29.html)
- <https://bdu.fstec.ru/vul/2024-06562>

**Краткое описание:** Выполнение произвольного кода в Google Chrome и Microsoft Edge

**Идентификатор уязвимости:** CVE-2024-10488

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Google Chrome и Microsoft Edge:  
Google Chrome: с версии 100.0.4896.60 по 130.0.6723.70  
Microsoft Edge: с версии 79.0.309.71 по 130.0.2849.56

**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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop\\_29.html](http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_29.html)

**Краткое описание:** Выполнение произвольного кода в Google Chrome и Microsoft Edge

**Идентификатор уязвимости:** CVE-2024-10487

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** Google Chrome и Microsoft Edge:  
Google Chrome: с версии 100.0.4896.60 по 130.0.6723.70  
Microsoft Edge: с версии 79.0.309.71 по 130.0.2849.56

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- [http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop\\_29.html](http://chromereleases.googleblog.com/2024/10/stable-channel-update-for-desktop_29.html)

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD и AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-9997

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

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

DWG Trueview: версии 2025

13

**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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0021>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1423/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD и AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-9996

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

DWG Trueview: версии 2025

14

**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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0021>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1424/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD и AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-9489

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

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

DWG Trueview: версии 2025

15

**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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0021>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1425/>

**Краткое описание:** Обход безопасности в Autodesk AutoCAD и AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8896

**Идентификатор программной ошибки:** CWE-908 Использование неинициализированных ресурсов

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

DWG Trueview: версии 2025

16

**Категория уязвимого продукта:** Прикладное программное обеспечение

**Способ эксплуатации:** Открытие пользователем специально созданного вредоносного файла.

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0021>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1426/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD и AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-7992

**Идентификатор программной ошибки:** CWE-121 Переполнение буфера в стеке

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

DWG Trueview: версии 2025

17 **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:N/I:N/A:N

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0021>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD и AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-7991

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

DWG Trueview: версии 2025

18 **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:N/I:N/A:N

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://autodesk.com/trust/security-advisories/adsk-sa-2024-0021>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8587

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

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

**Категория уязвимого продукта:** Прикладное программное обеспечение

19 **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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1441/>

**Краткое описание:** Получение конфиденциальной информации в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8588

**Идентификатор программной ошибки:** CWE-125 Чтение за пределами буфера

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025  
AutoCAD Architecture: версии 2025  
AutoCAD Electrical: версии 2025  
AutoCAD Mechanical: версии 2025  
AutoCAD MEP: версии 2025  
AutoCAD Plant 3D: версии 2025  
Autodesk Civil 3D: версии 2025  
Advance Steel: версии 2025

**Категория уязвимого продукта:** Прикладное программное обеспечение

20 **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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1439/>

**Краткое описание:** Получение конфиденциальной информации в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8589

**Идентификатор программной ошибки:** CWE-125 Чтение за пределами буфера

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025  
AutoCAD Architecture: версии 2025  
AutoCAD Electrical: версии 2025  
AutoCAD Mechanical: версии 2025  
AutoCAD MEP: версии 2025  
AutoCAD Plant 3D: версии 2025  
Autodesk Civil 3D: версии 2025  
Advance Steel: версии 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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1437/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8590

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

**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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1436/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8591

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

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025  
AutoCAD Architecture: версии 2025  
AutoCAD Electrical: версии 2025  
AutoCAD Mechanical: версии 2025  
AutoCAD MEP: версии 2025  
AutoCAD Plant 3D: версии 2025  
Autodesk Civil 3D: версии 2025  
Advance Steel: версии 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.

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1435/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8593

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

**Категория уязвимого продукта:** Прикладное программное обеспечение

24 **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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1434/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8594

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

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

**Категория уязвимого продукта:** Прикладное программное обеспечение

25 **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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1433/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8595

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

**Категория уязвимого продукта:** Прикладное программное обеспечение

26

**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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1432/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8597

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

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

**Категория уязвимого продукта:** Прикладное программное обеспечение

27 **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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1431/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8598

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

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025  
AutoCAD Architecture: версии 2025  
AutoCAD Electrical: версии 2025  
AutoCAD Mechanical: версии 2025  
AutoCAD MEP: версии 2025  
AutoCAD Plant 3D: версии 2025  
Autodesk Civil 3D: версии 2025  
Advance Steel: версии 2025

**Категория уязвимого продукта:** Прикладное программное обеспечение

28 **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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1430/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8599

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

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

**Категория уязвимого продукта:** Прикладное программное обеспечение

29 **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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1429/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8600

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

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

**Категория уязвимого продукта:** Прикладное программное обеспечение

30 **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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1440/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-9826

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

**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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1428/>

**Краткое описание:** Получение конфиденциальной информации в Autodesk AutoCAD and AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-9827

**Идентификатор программной ошибки:** CWE-125 Чтение за пределами буфера

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

**Категория уязвимого продукта:** Прикладное программное обеспечение

32 **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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1427/>

**Краткое описание:** Выполнение произвольного кода в Autodesk AutoCAD и AutoCAD-based products

**Идентификатор уязвимости:** CVE-2024-8596

**Идентификатор программной ошибки:** CWE-787 Запись за границами буфера

**Уязвимый продукт:** Autodesk AutoCAD и AutoCAD-based products:

Autodesk AutoCAD: версии 2025

AutoCAD Architecture: версии 2025

AutoCAD Electrical: версии 2025

AutoCAD Mechanical: версии 2025

AutoCAD MEP: версии 2025

AutoCAD Plant 3D: версии 2025

Autodesk Civil 3D: версии 2025

Advance Steel: версии 2025

**Категория уязвимого продукта:** Прикладное программное обеспечение

33 **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:N/I:N/A:H

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Требуется

**Дата выявления / Дата обновления:** 2024-10-30 / 2024-10-30

**Ссылки на источник:**

- <http://www.autodesk.com/trust/security-advisories/adsk-sa-2024-0019>
- <http://www.zerodayinitiative.com/advisories/ZDI-24-1438/>

**Краткое описание:** Выполнение произвольного кода в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-38415

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Выполнение произвольного кода в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-38419

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Выполнение произвольного кода в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-38422

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

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Выполнение произвольного кода в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-38421

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Выполнение произвольного кода в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-38423

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

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии

QCA9377: все версии  
QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии

SA4155P: все версии  
SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии

Snapdragon 480 5G Mobile Platform: все версии  
Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии

Snapdragon X62 5G Modem-RF System: все версии  
Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии

WCN6740: все версии  
WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

Краткое описание: Отказ в обслуживании в Qualcomm chipsets

Идентификатор уязвимости: CVE-2024-23385

Идентификатор программной ошибки: CWE-617 Несанкционированный вызов утверждения

Уязвимый продукт: Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Некорректная проверка входных 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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Выполнение произвольного кода в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-38408

**Идентификатор программной ошибки:** CWE-310 Уязвимости, связанные с криптографией

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Отказ в обслуживании в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-38403

**Идентификатор программной ошибки:** CWE-126 Чтение за границей буфера

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Некорректная проверка входных 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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Выполнение произвольного кода в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-38406

**Идентификатор программной ошибки:** CWE-367 Состояние гонки, связанное со временем проверки и временем использования

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Выполнение произвольного кода в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-38407

**Идентификатор программной ошибки:** CWE-367 Состояние гонки, связанное со временем проверки и временем использования

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Выполнение произвольного кода в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-38409

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

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии

QCA9377: все версии  
QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии

SA4155P: все версии  
SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии

Snapdragon 480 5G Mobile Platform: все версии  
Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии

Snapdragon X62 5G Modem-RF System: все версии  
Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии

WCN6740: все версии  
WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Выполнение произвольного кода в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-38410

**Идентификатор программной ошибки:** CWE-121 Переполнение буфера в стеке

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Выполнение произвольного кода в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-38424

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Отказ в обслуживании в Qualcomm chipsets

**Идентификатор уязвимости:** CVE-2024-33068

**Идентификатор программной ошибки:** CWE-416 Использование после освобождения

**Уязвимый продукт:** Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Некорректная проверка входных 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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

Краткое описание: Отказ в обслуживании в Qualcomm chipsets

Идентификатор уязвимости: CVE-2024-38405

Идентификатор программной ошибки: CWE-126 Чтение за границей буфера

Уязвимый продукт: Qualcomm chipsets:  
AR8035: все версии  
CSRA6620: все версии  
CSRA6640: все версии  
FastConnect 6200: все версии  
FastConnect 6700: все версии  
FastConnect 6800: все версии  
FastConnect 6900: все версии  
FastConnect 7800: все версии  
Flight RB5 5G Platform: все версии  
MDM9628: все версии  
QAM8295P: все версии  
QCA6174A: все версии  
QCA6391: все версии  
QCA6421: все версии  
QCA6426: все версии  
QCA6431: все версии  
QCA6436: все версии  
QCA6564A: все версии  
QCA6564AU: все версии  
QCA6574: все версии  
QCA6574A: все версии  
QCA6574AU: все версии  
QCA6595: все версии  
QCA6595AU: все версии  
QCA6696: все версии  
QCA6698AQ: все версии  
QCA8081: все версии  
QCA8337: все версии  
QCA9377: все версии

QCM2150: все версии  
QCM2290: все версии  
QCM4290: все версии  
QCM4490: все версии  
QCM5430: все версии  
QCM6490: все версии  
QCM8550: все версии  
QCN6024: все версии  
QCN9011: все версии  
QCN9012: все версии  
QCN9024: все версии  
QCN9274: все версии  
QCS2290: все версии  
QCS410: все версии  
QCS4290: все версии  
QCS4490: все версии  
QCS5430: все версии  
QCS610: все версии  
QCS6490: все версии  
QCS7230: все версии  
QCS8250: все версии  
QCS8550: все версии  
QCS9100: все версии  
QRB5165M: все версии  
QRB5165N: все версии  
QSM8250: все версии  
QSM8350: все версии  
Qualcomm 215 Mobile Platform: все версии  
Qualcomm Video Collaboration VC1 Platform: все версии  
Qualcomm Video Collaboration VC3 Platform: все версии  
Qualcomm Video Collaboration VC5 Platform: все версии  
Robotics RB5 Platform: все версии  
SA4150P: все версии  
SA4155P: все версии

SA6145P: все версии  
SA6150P: все версии  
SA6155P: все версии  
SA8145P: все версии  
SA8150P: все версии  
SA8155P: все версии  
SA8195P: все версии  
SA8295P: все версии  
SA8530P: все версии  
SA8540P: все версии  
SA9000P: все версии  
SD 8 Gen1 5G: все версии  
SD660: все версии  
SD670: все версии  
SD865 5G: все версии  
SD888: все версии  
SDX55: все версии  
SDX61: все версии  
SG8275P: все версии  
SM4125: все версии  
SM6370: все версии  
SM7250P: все версии  
SM7315: все версии  
SM7325P: все версии  
SM8550P: все версии  
SM8635: все версии  
SM8750: все версии  
SM8750P: все версии  
Smart Audio 400 Platform: все версии  
Snapdragon 4 Gen 1 Mobile Platform: все версии  
Snapdragon 4 Gen 2 Mobile Platform: все версии  
Snapdragon 439 Mobile Platform: все версии  
Snapdragon 460 Mobile Platform: все версии  
Snapdragon 480 5G Mobile Platform: все версии

Snapdragon 480+ 5G Mobile Platform (SM4350-AC): все версии  
Snapdragon 660 Mobile Platform: все версии  
Snapdragon 662 Mobile Platform: все версии  
Snapdragon 670 Mobile Platform: все версии  
Snapdragon 680 4G Mobile Platform: все версии  
Snapdragon 685 4G Mobile Platform (SM6225-AD): все версии  
Snapdragon 690 5G Mobile Platform: все версии  
Snapdragon 695 5G Mobile Platform: все версии  
Snapdragon 710 Mobile Platform: все версии  
Snapdragon 750G 5G Mobile Platform: все версии  
Snapdragon 765 5G Mobile Platform (SM7250-AA): все версии  
Snapdragon 765G 5G Mobile Platform (SM7250-AB): все версии  
Snapdragon 768G 5G Mobile Platform (SM7250-AC): все версии  
Snapdragon 778G 5G Mobile Platform: все версии  
Snapdragon 778G+ 5G Mobile Platform (SM7325-AE): все версии  
Snapdragon 780G 5G Mobile Platform: все версии  
Snapdragon 782G Mobile Platform (SM7325-AF): все версии  
Snapdragon 7c+ Gen 3 Compute: все версии  
Snapdragon 8 Gen 1 Mobile Platform: все версии  
Snapdragon 8 Gen 2 Mobile Platform: все версии  
Snapdragon 8 Gen 3 Mobile Platform: все версии  
Snapdragon 8+ Gen 1 Mobile Platform: все версии  
Snapdragon 8+ Gen 2 Mobile Platform: все версии  
Snapdragon 865 5G Mobile Platform: все версии  
Snapdragon 865+ 5G Mobile Platform (SM8250-AB): все версии  
Snapdragon 870 5G Mobile Platform (SM8250-AC): все версии  
Snapdragon 888 5G Mobile Platform: все версии  
Snapdragon 888+ 5G Mobile Platform (SM8350-AC): все версии  
Snapdragon AR2 Gen 1 Platform: все версии  
Snapdragon Auto 5G Modem-RF: все версии  
Snapdragon W5+ Gen 1 Wearable Platform: все версии  
Snapdragon X12 LTE Modem: все версии  
Snapdragon X55 5G Modem-RF System: все версии  
Snapdragon X62 5G Modem-RF System: все версии

Snapdragon X65 5G Modem-RF System: все версии  
Snapdragon XR1 Platform: все версии  
Snapdragon XR2 5G Platform: все версии  
Snapdragon XR2+ Gen 1 Platform: все версии  
SSG2115P: все версии  
SSG2125P: все версии  
SW5100: все версии  
SW5100P: все версии  
SXR1120: все версии  
SXR1230P: все версии  
SXR2130: все версии  
SXR2230P: все версии  
SXR2250P: все версии  
TalynPlus: все версии  
Vision Intelligence 400 Platform: все версии  
WCD9326: все версии  
WCD9335: все версии  
WCD9341: все версии  
WCD9370: все версии  
WCD9375: все версии  
WCD9380: все версии  
WCD9385: все версии  
WCD9390: все версии  
WCD9395: все версии  
WCN3615: все версии  
WCN3660B: все версии  
WCN3680: все версии  
WCN3680B: все версии  
WCN3910: все версии  
WCN3950: все версии  
WCN3980: все версии  
WCN3988: все версии  
WCN3990: все версии  
WCN6740: все версии

WCN6755: все версии  
WCN7860: все версии  
WCN7861: все версии  
WCN7880: все версии  
WCN7881: все версии  
WSA8810: все версии  
WSA8815: все версии  
WSA8830: все версии  
WSA8832: все версии  
WSA8835: все версии  
WSA8840: все версии  
WSA8845: все версии  
WSA8845H: все версии

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Некорректная проверка входных 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

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-11-04 / 2024-11-04

**Ссылки на источник:**

- <http://docs.qualcomm.com/product/publicresources/securitybulletin/november-2024-bulletin.html>

**Краткое описание:** Выполнение произвольного кода в Siemens InterMesh Subscriber Devices

**Идентификатор уязвимости:** CVE-2024-47904

**Идентификатор программной ошибки:** CWE-266 Некорректное назначение привилегий

**Уязвимый продукт:** Siemens InterMesh Subscriber Devices:  
InterMesh 7177 Hybrid 2.0 Subscriber: до версии 8.2.12  
InterMesh 7707 Fire Subscriber: до версии 7.2.12

**Категория уязвимого продукта:** Телекоммуникационное оборудование

**Способ эксплуатации:** Не определено

**Последствия эксплуатации:** Выполнение произвольного кода

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

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

**Вектор атаки:** Локальный

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-31 / 2024-10-31

**Ссылки на источник:**

- <http://cert-portal.siemens.com/productcert/html/ssa-333468.html>

**Краткое описание:** Выполнение произвольного кода в Siemens InterMesh Subscriber Devices

**Идентификатор уязвимости:** CVE-2024-47901

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

**Уязвимый продукт:** Siemens InterMesh Subscriber Devices:  
InterMesh 7177 Hybrid 2.0 Subscriber: до версии 8.2.12  
InterMesh 7707 Fire Subscriber: до версии 7.2.12

**Категория уязвимого продукта:** Телекоммуникационное оборудование

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

50 **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:N/A:N

**Вектор атаки:** Сетевой

**Взаимодействие с пользователем:** Отсутствует

**Дата выявления / Дата обновления:** 2024-10-31 / 2024-10-31

**Ссылки на источник:**

- <http://cert-portal.siemens.com/productcert/html/ssa-333468.html>