

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220302.5 | 2 марта 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в PJSIP

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	pjsip: 0.5.0.1 - 2.11.1
Дата выявления	02 марта 2022 г.
Дата обновления	02 марта 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-43299 CVE-2021-43300 CVE-2021-43301	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-121: Переполнение буфера в стеке</p> <p>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.</p>	9.8

<p>MITRE: CVE-2021-43302</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику вызвать отказ в обслуживании целевой системы. Уязвимость обусловлена граничным условием.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C</p> <p>CWE-125: Чтение за пределами буфера</p> <p>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.</p>	<p>7.5</p>
<p>MITRE: CVE-2021-43303</p>	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-119: Выполнение операций за пределами буфера памяти</p> <p>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.</p>	<p>9.8</p>

Ссылки на источники

- <https://www.cybersecurity-help.cz/vdb/SB2022030212>
- <http://github.com/pjsip/pjproject/security/advisories/GHSA-qcww-h34v-c7r9>
- <http://jfrog.com/blog/jfrog-discloses-5-memory-corruption-vulnerabilities-in-pjsip-a-popular-multimedia-library/>