

# НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР  
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220305.8 | 5 марта 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Множественные уязвимости в IPCOMM ipDIO

Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	ipDIO: 3.9
Дата выявления	04 марта 2022 г.
Дата обновления	04 марта 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-24915	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе посредством отправки специально созданного запроса. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H/E:U/RL:U/RC:C</p> <p>CWE-94: Некорректное управление генерированием кода (внедрение кода)</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>	8.0

MITRE: CVE-2022-22985	<p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольной код в целевой системе посредством отправки специально созданного запроса. Уязвимость обусловлена некорректной проверкой входных данных.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C</p> <p>CWE-94: Некорректное управление генерированием кода (внедрение кода)</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>	8.8
--------------------------	--	-----

Ссылки на источники	<p><a href="https://www.cybersecurity-help.cz/vdb/SB2022030402">https://www.cybersecurity-help.cz/vdb/SB2022030402</a></p> <p><a href="http://ics-cert.us-cert.gov/advisories/icsa-22-062-01">http://ics-cert.us-cert.gov/advisories/icsa-22-062-01</a></p>	
---------------------	---	--