

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220822.12 | 22 августа 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Множественные уязвимости в FreeBSD

Категория уязвимого продукта	UNIX-подобные операционные системы
Уязвимый продукт	FreeBSD: 13.0 - 13.1
Дата выявления	13 августа 2022 г.
Дата обновления	13 августа 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2022-23092	<p>Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти.</p> <p>CVSSv3.0: AV:N/AC:L/PR:L/UI:N/S:C/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>	9.9

MITRE: CVE-2022-23090	<p>Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код с привилегиями «root». Уязвимость обусловлена ошибкой использования после освобождения.</p> <p>CVSSv3.0: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C</p> <p>CWE-416: Использование после освобождения</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>http://www.freebsd.org/security/advisories/FreeBSD-SA-22:12.lib9p.asc</p> <p>http://www.freebsd.org/security/advisories/FreeBSD-SA-22:10.aio.asc</p>	