

# 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)

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20221202.1 | 2 декабря 2022 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

## Выполнение произвольного кода в FreeBSD

Идентификатор уязвимости	MITRE: CVE-2022-23093
Идентификатор программной ошибки	CWE-121: Переполнение буфера в стеке
Описание уязвимости	Эксплуатация уязвимости позволяет выполнить произвольный код в целевой системе посредством отправки специально сформированного ICMP-запроса. Уязвимость обусловлена ошибкой границ памяти.
Категория уязвимого продукта	UNIX-подобные операционные системы
Уязвимый продукт	FreeBSD: 12.0 - 13.1
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.
Дата выявления	30 ноября 2022 г.
Дата обновления	30 ноября 2022 г.
Оценка критичности уязвимости (CVSSv3.1)	Неопределено
Вектор атаки (AV)	Неопределено
Сложность эксплуатации уязвимости (AC)	Неопределено
Необходимый уровень привилегий (PR)	Неопределено
Необходимость взаимодействия с пользователем (UI)	Неопределено
Масштаб последствий эксплуатации уязвимости (S)	Неопределено

Влияние на конфиденциальность (C)	Неопределено
Влияние на целостность (I)	Неопределено
Влияние на доступность (A)	Неопределено
Степень зрелости доступных средств эксплуатации	Неопределено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Неопределено

---

Ссылки на источники

<http://www.freebsd.org/security/advisories/FreeBSD-SA-22:15.ping.asc>