

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20200514.1 | 14 мая 2020 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Повреждение памяти в межсетевом экране ipfw ОС FreeBSD

| | |
|------------------------------|---|
| Категория уязвимого продукта | Средства защиты информации |
| Уязвимое ПО | FreeBSD: 11.0, 11.1, 11.2, 11.3, 12.0, 12.1 |
| Дата выявления | 12 мая 2020 г. |
| Дата обновления | 12 мая 2020 г. |

| Идентификатор уязвимости | Описание уязвимости | Базовый уровень CVSS |
|--------------------------|---|----------------------|
| MITRE: CVE-2020-7454 | <p>Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально созданного вредоносного пакета. Уязвимость обусловлена некорректной проверкой длины пакета в библиотеке libalias (3) при обработке сетевых пакетов.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-787: Запись за границами буфера</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p> | 10.0 |

| | | |
|-------------------------|--|-----|
| MITRE: CVE-2020-7455 | <p>Эксплуатация уязвимости позволяет удаленному злоумышленнику получить доступ к данным в памяти ядра или процесса natd (Network Address Translation) в целевой системе посредством отправки специально созданного вредоносного FTP-пакета. Уязвимость обусловлена граничным условием в библиотеке libalias (3) при расчете длины в FTP-пакетах.</p> <p>CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N/E:U/RL:O/RC:C CWE-125: Чтение за пределами буфера</p> <p>Рекомендации по устранению: обновить программное обеспечение.</p> | 8.6 |
|-------------------------|--|-----|

| | | |
|---------------------|--|--|
| Ссылки на источники | <p>https://www.freebsd.org/security/advisories/FreeBSD-SA-20:12.libalias.asc https://www.freebsd.org/security/advisories/FreeBSD-SA-20:13.libalias.asc https://www.cybersecurity-help.cz/vdb/SB2020051273</p> | |
|---------------------|--|--|