

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20191230.1 | 30 декабря 2019 г.

Уровень опасности: **ВЫСОКИЙ**

Наличие обновления: **ЕСТЬ**

Повышение привилегий в динамическом загрузчике ОС OpenBSD

| | |
|---|--|
| Идентификатор уязвимости | MITRE: CVE-2019-19726 |
| Идентификатор программной ошибки | CWE-269: Некорректное управление привилегиями |
| Описание уязвимости | Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить привилегии в целевой системе посредством ограничения ресурсов памяти в переменной RLIMIT_DATA и запуска исполняемого файла chpass или passwd. Уязвимость обусловлена некорректной работой динамического загрузчика ld.so с переменной LD_LIBRARY_PATH. |
| Категория уязвимого продукта | Unix-подобные операционные системы и их компоненты |
| Уязвимое ПО | OpenBSD до v6.6 |
| Рекомендации по устранению | Обновить программное обеспечение |
| Дата выявления | 11 декабря 2019 г. |
| Дата обновления | 27 декабря 2019 г. |
| Оценка критичности уязвимости (CVSSv3) | 7.8 AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:O/RC:C |
| Вектор атаки (AV) | Локальный (L) |
| Сложность эксплуатации уязвимости (AC) | Низкая (L) |
| Необходимый уровень привилегий (PR) | Низкий (L) |
| Необходимость взаимодействия с пользователем (UI) | Отсутствует (N) |
| Масштаб последствий эксплуатации уязвимости (S) | Не изменяется (U) |

Влияние на конфиденциальность (C)

Высокое (H)

Влияние на целостность (I)

Высокое (H)

Влияние на доступность (A)

Высокое (H)

Степень зрелости доступных средств эксплуатации (E)

Концептуальное подтверждение (P)

Наличие средств устранения уязвимости (RL)

Официальное решение (O)

Достоверность сведений об уязвимости (RC)

Сведения подтверждены (C)

Ссылки на источники

<https://packetstormsecurity.com/files/155658/Qualys-Security-Advisory-OpenBSD-Dynamic-Loader-Privilege-Escalation.html>

<https://nvd.nist.gov/vuln/detail/CVE-2019-19726>

<https://packetstormsecurity.com/files/155764/OpenBSD-Dynamic-Loader-chpass-Privilege-Escalation.html>

<https://www.openbsd.org/errata66.html>

<https://www.opennet.ru/opennews/art.shtml?num=52012>