НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210722.5 | 22 июля 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в Linux kernel

Идентификатор уязвимости	MITRE: CVE-2021-33909
Идентификатор программной ошибки	CWE-190: Целочисленное переполнение или циклический возврат
Описание уязвимости	Эксплуатация уязвимости позволяет локальному аутентифицированному злоумышленнику повысить свои привилегии в целевой системе посредством размещения файла с именем превышающим определенную длину. Уязвимость обусловлена целочисленным переполнением буфера в функции vmalloc().
Категория уязвимого продукта	UNIX-подобные операционные системы
Уязвимый продукт	Linux kernel: до v5.13.4
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	21 июля 2021 г.
Дата обновления	21 июля 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	8.8 AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
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)	Изменяется (C)
Влияние на конфиденциальность (C)	Высокое (H)

Влияние на целостность (I)	Высокое (H)
Влияние на доступность (A)	Высокое (H)
Степень зрелости доступных средств эксплуатации	Концептуальное подтверждение
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021072106 https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.4 https://github.com/torvalds/linux/commit/8cae8cd89f05f6de223d63e6d15e31c8ba9cf53b https://www.openwall.com/lists/oss-security/2021/07/20/1