НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20230404.2 | 4 апреля 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в Linux

Идентификатор уязвимости	MITRE: CVE-2023-28772
Идентификатор программной ошибки	CWE-120: Копирование содержимого буфера без проверки размера входных данных (классическое переполнение буфера)
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти.
Категория уязвимого продукта	Unix-подобные операционные системы и их компоненты
Уязвимый продукт	Linux: от 4.0 до 4.4.275 включительно от 4.5 до 4.9.275 включительно от 4.10 до 4.14.239 включительно от 4.15 до 4.19.197 включительно от 4.20 до 5.4.132 включительно от 5.5 до 5.10.50 включительно от 5.11 до 5.12.17 включительно от 5.13.0 до 5.13.2 включительно
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	23 марта 2023 г.
Дата обновления	27 марта 2023 г.
Оценка критичности уязвимости (CVSSv3.1)	7.8 CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/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)	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	Не определено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Не определено
Ссылки на источники	https://nvd.nist.gov/vuln/detail/CVE-2023-28772 https://github.com/torvalds/linux/commit/d3b16034a24a112bb83aeb669ac5b9b01f744bb7 https://lore.kernel.org/lkml/20210625122453.5e2fe304@oasis.local.home/ https://cdn.kernel.org/pub/linux/kernel/v5.x/ChangeLog-5.13.3 https://lore.kernel.org/all/20210626032156.47889-1-yun.zhou@windriver.com/T/#u https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-28772 https://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git/commit/?id=d3b16034a24a112bb83aeb669ac5b9b01f744bb7 https://lore.kernel.org/all/20210626032156.47889-1-yun.zhou@windriver.com/T/#u https://bdu.fstec.ru/vul/2023-01796