НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20230331.1 | 31 марта 2023 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Повышение привилегий в Midgard GPU Kernel Driver

Идентификатор уязвимости	MITRE: CVE-2022-22706
Идентификатор программной ошибки	CWE-787: Запись за границами буфера
Описание уязвимости	Эксплуатация уязвимости позволяет аутентифицированному локальному злоумышленнику выполнить произвольный код с повышенными привилегиями в целевой системе. Уязвимость обусловлена ошибкой границ памяти.
Категория уязвимого продукта	Универсальные компоненты и библиотеки
Уязвимый продукт	Midgard GPU Kernel Driver: до r32p0 Bifrost GPU Kernel Driver: до r36p0 Valhall GPU Kernel Driver: до r36p0
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 марта 2023 г.
Дата обновления	30 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	http://developer.arm.com/support/arm-security-updates/mali-gpu-kernel-driver http://blog.google/threat-analysis-group/spyware-vendors-use-0-days-and-n-days-against-popular-platforms/