НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20210927.5 | 27 сентября 2021 г.

Уровень опасности: ВЫСОКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольных команд в Huawei FusionCompute

Идентификатор уязвимости	MITRE: CVE-2021-37106
Идентификатор программной ошибки	CWE-77: Некорректная нейтрализация специальных элементов, используемых в командах (внедрение команд)
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному аутентифицированному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально созданных данных. Уязвимость обусловлена некорректной проверкой входных данных в сервисном модуле CMA.
Категория уязвимого продукта	Прикладное программное обеспечение
Уязвимый продукт	FusionCompute: 6.3.0, 6.3.1, 6.5.0, 8.0.0
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	23 сентября 2021 г.
Дата обновления	23 сентября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	7.2 AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H
Вектор атаки (AV)	Сетевой (N)
Сложность эксплуатации уязвимости (AC)	Низкая (L)
Необходимый уровень привилегий (PR)	Высокий (H)
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	Наличие не подтверждено
Наличие средств устранения уязвимости	Официальное решение
Достоверность сведений об уязвимости	Сведения подтверждены
Ссылки на источники	https://www.cybersecurity-help.cz/vdb/SB2021092302 https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210922-01-commandinjection-en