НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211119.2 | 19 ноября 2021 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: ЕСТЬ

Выполнение произвольного кода в QNAP QTS и QuTS hero

Идентификатор уязвимости	Не определен
Идентификатор программной ошибки	CWE-122: Переполнение буфера в динамической памяти
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена ошибкой границ памяти при включенном протоколе AFP (Apple File Protocol).
Категория уязвимого продукта	Телекоммуникационное оборудование
Уязвимый продукт	QNAP QTS: до 4.3.3.1799, 4.3.6.1831, 4.5.4.1800, 5.0.0.1808 QuTS hero: до h4.5.4.1813 build 20211006, h5.0.0.1844 build 20211105
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	19 ноября 2021 г.
Дата обновления	19 ноября 2021 г.
Оценка критичности уязвимости (CVSSv3.1)	9.8 AV:N/AC:L/PR:N/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)	Отсутствует (N)
Необходимость взаимодействия с пользователем (UI)	Отсутствует (N)
Масштаб последствий эксплуатации	Не изменяется (U)

уязвимости (S)	
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/SB2021111907 http://www.qnap.com/en/security-advisory/qsa-21-50