

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20220211.3 | 11 февраля 2022 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в QNAP Kazoo Server

Идентификатор уязвимости	MITRE: CVE-2021-38679
Идентификатор программной ошибки	CWE-287: Некорректная аутентификация
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена некорректной работой процесса аутентификации.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	QNAP QTS: 4.5.3 QuTS hero: h4.5.3 Kazoo Server: до 4.11.22
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	11 февраля 2022 г.
Дата обновления	11 февраля 2022 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 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/SB2022021101 http://www.gnap.com/en/security-advisory/qs-a-22-01