

НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru

E-mail: threats@cert.gov.ru

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТИ

VULN-20211217.7 | 17 декабря 2021 г.

Уровень опасности: **КРИТИЧЕСКИЙ**

Наличие обновления: **ЕСТЬ**

Выполнение произвольного кода в QNAP NAS Surveillance Station

Идентификатор уязвимости	MITRE: CVE-2021-38687
Идентификатор программной ошибки	CWE-121: Переполнение буфера в стеке
Описание уязвимости	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе посредством отправки специально сформированного запроса. Уязвимость обусловлена ошибкой границ памяти.
Категория уязвимого продукта	Серверное программное обеспечение и его компоненты
Уязвимый продукт	Surveillance Station: до 5.1.5.4.5
Рекомендации по устранению	Обновить программное обеспечение
Дата выявления	9 декабря 2021 г.
Дата обновления	9 декабря 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 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/SB2021120917>
<http://www.qnap.com/en/security-advisory/qlsa-21-46>