НКЦКИ

НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

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

УВЕДОМЛЕНИЕ ОБ УЯЗВИМОСТЯХ

VULN-20220426.2 | 26 апреля 2022 г.

Уровень опасности: КРИТИЧЕСКИЙ

Наличие обновления: НЕТ

Множественные уязвимости в QuTS hero Netatalk и QNAP QuTScloud Netatalk

Категория уязвимого продукта	Unix-подобные операционные системы и их компоненты
Уязвимый продукт	QuTScloud: c5.0.0.1919 20220119 - c5.0.1.1998 20220408 QuTS hero: h4.5.0.1279 build 20200421 - h5.0.0.1986 Build 20220324
Дата выявления	25 апреля 2022 г.
Дата обновления	25 апреля 2022 г.

Идентификатор уязвимости	Описание уязвимости	Базовый уровень CVSS
MITRE: CVE-2021-31439	Эксплуатация уязвимости позволяет злоумышленнику из смежной сети выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-122: Переполнение буфера в динамической памяти Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	8.8

MITRE: CVE-2022-23121	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольные команды в целевой системе посредством отправки специально сформированных данных. Уязвимость обусловлена некорректной обработкой исключительных условий в функции. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:U/RC:C CWE-755: Некорректная обработка исключений Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	9.8
MITRE: CVE-2022-23122	Эксплуатация уязвимости позволяет удаленному злоумышленнику прочитать содержимое памяти в целевой системе. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-121: Переполнение буфера в стеке Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	9.8
MITRE: CVE-2022-23123	Эксплуатация уязвимости позволяет удаленному злоумышленнику прочитать содержимое памяти в целевой системе. Уязвимость обусловлена граничным условием в методе. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-125: Чтение за пределами буфера Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	7.5
MITRE: CVE-2022-23124	Эксплуатация уязвимости позволяет удаленному злоумышленнику прочитать содержимое памяти в целевой системе. Уязвимость обусловлена граничным условием в методе. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C CWE-125: Чтение за пределами буфера Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	7.5

MITRE: CVE-2022-23125	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-121: Переполнение буфера в стеке Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	9.8
MITRE: CVE-2022-0194	Эксплуатация уязвимости позволяет удаленному злоумышленнику выполнить произвольный код в целевой системе. Уязвимость обусловлена ошибкой границ памяти. CVSSv3.0: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RL:O/RC:C CWE-121: Переполнение буфера в стеке Рекомендации по устранению: Ограничить доступ к уязвимому продукту средствами межсетевого экранирования или другими административными мерами.	9.8

Ссылки на источники	http://www.qnap.com/en/security-advisory/qsa-22-12