Kalteberatasunak QNAP produktuetan

CYBERZAINTZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA
GOBIERNO VASCO

EDUKI-TAULA

Erantzukizunetik salbuesteko klausula

Salmenta debekatzeko klausula

1. Laburpen exekutiboa

Qnapek segurtasun-abisu bat argitaratu du **3 kalteberatasun jorratzeko, 1 larritasun kritikokoa** (CVE-2024-21899) eta **bi larritasun ertainekoak** (CVE-2024-21900 eta CVE-2024-21901). Akatsek **QTS, QuTS hero, QuTScloud eta myQNAPcloud** produktuei eragiten diete.

Kalteberatasun kritikoa ustiatuz gero, arriskuan jar liteke sare bidezko sistema eta kaltetutako sistemen konfidentzialtasunean, osotasunean eta eskuragarritasunean eragina izan dezakete.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion eguneratzeak eta arintze-neurriak, eta, horrela, akats nabarmenak zuzendu ditu. Beraz, kalteberatasun hori eta beste batzuk prebenitzeko, gomendagarria da sistemak eta aplikazioak beti eskuragarri dagoen azken bertsioarekin gaurkotuta izatea.

2. Kaltetutako baliabideak

Honako hauek dira kaltetutako produktuak:

- QTS 5.1.x.
- QTS 4.5.x.
- QuTS hero h5.1.x.
- QuTS hero h4.5.x.
- QuTScloud c5.x.
- myQNAPcloud 1.0.

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasunaren xehetasunak hauek dira:

CVE-2024-21899: egiaztatze okerreko kalteberatasunak QNAP sistema eragilearen hainbat bertsiori eragiten die. Kalteberatasun hori ustiatuz gero, eragile gaiztoek arriskuan jar dezakete sistemaren segurtasuna sarearen bitartez.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

CWE-287: Improper Authentication

Oinarrizko CVSSa: **9.8**

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna**: Baxua
- **Beharrezko pribilegioak: Bat ere ez**
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Irismena**: Aldaketarik gabe
- **Konfidentzialtasuna Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

4. Arintzea / Konponbidea

QNAPek sistema eta aplikazioak azken bertsioarekin modu erregularrean eguneratzea gomendatzen du, kalteberetasun horiek zuzentzeko.

Kalteberatasun horiek eragindako tresnak eguneratzeko moduak eskuragarri daude abisuan bertan, eta hauek dira:

- QTS 5.1.x, eguneratu QTS 5.1.3.2578 bertsiora, 20231110 konpilaziora eta ondorengoetara.
- QTS 4.5.x, eguneratu QTS 4.5.4.2627 bertsiora, 20231225 konpilaziora eta ondorengoetara.
- QuTS hero h5.1.x, eguneratu h5.1.3.2578 bertsiora, 20231110 konpilaziora eta ondorengoetara.
- QuTS hero h4.5.x, eguneratu h4.5.4.2626 bertsiora, 20231225 konpilaziora eta ondorengoetara.
- QuTScloud c5.x, eguneratu QuTScloud c5.1.5.265 bertsiora eta ondorengoetara.
- myQNAPcloud 1.0.x, eguneratu myQNAPcloud 1.0.52 bertsiora (2023/11/24) eta ondorengoetara.

5. Erreferentzia gehigarriak

- Segurtasun-abisua.
- CVE-2024-21899.
- CVE-2024-21900.
- CVE-2024-21901.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY