



Kalteberatasunak QNAP produktuetan

CYBERZAINZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus



EDUKI-TAULA

| | |
|----------------------------------|---|
| 1. Resumen ejecutivo..... | 3 |
| 2. Recursos afectados | 4 |
| 3. Análisis técnico | 5 |
| 4. Mitigación / Solución..... | 6 |
| 5. Referencias Adicionales | 7 |

Erantzukizunetik salbuesteko klausula

Dokumentu hau Zibersegurtasunaren Euskal Agentziak erakundeen eta herritar interesatuen segurtasunaren alde beharrezkotzat jotzen dituen alertak gizarteratzeko helburuz sortu da. Zibersegurtasunaren Euskal Agentzia ezin da jo, inola ere, Zibersegurtasunerako Euskal Agentziaren webgunean emandako informazioaren edo erreferentzia egiten zaien teknologien erabilerak eragin ditzaketen kalteen erantzuletzat, ezta kanpoko web-orrialdeetarako esteka bidez sartutako bestelako informazioaren, software produktuen edo Zibersegurtasunaren Euskal Agentziaren webgunean edo alertan ager daitezkeen beste edozein informazioaren erantzuletzat ere. Edonola ere, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak iritzi eta gomendioak dira, hemen bildutako terminoekin bat etorrita, eta emandako informazioaren ondorioz ezingo da eragin juridiko loteslerik sortu.

Salmenta debekatzeko klausula

Gutziz debekatuta dago saltzea edo edozein etekin ekonomiko lortzea, baina horrek ez du eragotziko dokumentu hau kopiatzeko, banatzeko, zabaltzeko edo gizarteratzeko aukera.

1. Laburpen exekutiboa

Qnapek [segurtasun-abisu](#) bat argitaratu du **3 kalteberatasun jorrazeko, 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 ustatuz gero, arriskuan jar liteke sare bidezko sistema eta kaltetutako sistemen konfidentziasunean, 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 tekniko

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**
- **Konfidentziasuna: Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

4. Arintzea / Konponbidea

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

Kalteberetasun 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.
- QuTScldoud c5.x, eguneratu QuTScldoud 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.](#)

