



BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits QNAP
Numéro de Référence	44351710/23
Date de Publication	17 Octobre 2023
Risque	Important
Impact	Important

Systemes affectés

- Container Station versions 5..6.x antérieures à 2.6.7.44
- QTS hero versions h4.5.x antérieures à h4.5.4.2476 build 20230728
- QTS hero versions h5.0.x antérieures à h5.0.1.2515 build 20230907
- QTS hero versions h5.1.x antérieures à h5.1.0.2424 build 20230609
- QTS versions 4.5.x antérieures à 4.5.4.2467 build 20230718
- QTS versions 5.0.x antérieures à 5.0.1.2425 build 20230609
- QTS versions 5.1.x antérieures à 5.1.0.2444 build 20230629
- QuTScld versions c5.x antérieures à c5.1.0.2498
- Video Station versions 5.7.x antérieures à 5.7.0 (2023/07/27)

Identificateurs externes

CVE-2023-32970 CVE-2023-32973 CVE-2023-32974 CVE-2023-32976 CVE-2023-34975
CVE-2023-34976 CVE-2023-34977

Bilan de la vulnérabilité

QNAP annonce la disponibilité de mises à jour de sécurité permettant la correction de plusieurs vulnérabilités affectant ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, de contourner les mesures de sécurité ou de causer un déni de service.

Solution

Veillez se référer aux bulletins de sécurité de QNAP pour installer les mises à jour.

Risques

- Exécution de code arbitraire
- Contournement de mesures de sécurité
- Déni de service

Référence

Bulletins de sécurité de QNAP :

- <https://www.qnap.com/fr-fr/security-advisory/qa-23-41>
- <https://www.qnap.com/fr-fr/security-advisory/qa-23-42>
- <https://www.qnap.com/fr-fr/security-advisory/qa-23-44>
- <https://www.qnap.com/fr-fr/security-advisory/qa-23-52>