



BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits QNAP
Numéro de Référence	45900602/24
Date de Publication	06 Février 2024
Risque	Critique
Impact	Critique

Systemes affectés

- QTS 5.1.x version antérieure à QTS 5.1.4.2596 build 20231128
- QTS 4.5.x antérieure à QTS 4.5.4.2627 build 20231225
- QuTS hero h5.1.x antérieure à QuTS hero h5.1.4.2596 build 20231128
- QuTS hero h4.5.x antérieure à QuTS hero h4.5.4.2626 build 20231225
- QuTScloud 5.x antérieure à QuTScloud c5.1.5.2651
- Qsync Central 4.3.x antérieure à Qsync Central 4.3.0.11 (2024/01/11)
- Qsync Central 4.4.x antérieure à Qsync Central 4.4.0.15 (2024/01/04)

Identificateurs externes

- CVE-2023-45025, CVE- 2023-39297 CVE-2023-47564

Bilan de la vulnérabilité

QNAP Systems a publié des correctifs de sécurité pour des vulnérabilités de haute sévérité (CVE-2023-45025, CVE- 2023-39297 et CVE-2023-47564) affectant ses systèmes d'exploitation QTS et Qsync Central. Ces vulnérabilités sont des failles d'injection de commande au niveau du système d'exploitation et une vulnérabilité d'attribution incorrecte de permission pour les ressources critiques qui pourraient permettre aux attaquants d'exécuter des com-

mandes arbitraires sur les appareils affectés, ce qui pourrait conduire à une compromission complète du système.

Solution

Veillez se référer au bulletin de sécurité QNAP du 03 Février 2024.

Risque

- Injection des commandes arbitraires,
- Prise de contrôle du système affecté
- Atteinte à la confidentialité des données,

Annexe

Bulletin de sécurité QNAP du 03 Février 2024:

- <https://www.qnap.com/en/security-advisory/qa-23-47>
- <https://www.qnap.com/en/security-advisory/qa-23-30>