



## BULLETIN DE SECURITE

|                            |  |
|----------------------------|--|
| <b>Titre</b>               | Vulnérabilités affectant des produits QNAP |
| <b>Numéro de Référence</b> | 43070108/23                                |
| <b>Date de Publication</b> | 01 Aout 2023                               |
| <b>Risque</b>              | Important                                  |
| <b>Impact</b>              | Important                                  |

### Systemes affectés

- QTS versions antérieures à la version 4.5.4.2280 build 20230112
- QTS versions antérieures à la version 5.0.1.2277 build 20230112
- QVPN Device Client pour Windows versions antérieures à la version 2.0.0.1316
- QVR Pro Appliance versions antérieures à la version 2.3.1.0476
- QuTS hero versions antérieures à la version h4.5.4.2374 build 20230417
- QuTS hero versions antérieures à la version h5.0.1.2277 build 20230112
- QuTScloud versions antérieures à la version c5.0.1.2374 build 20230419

### Identificateurs externes

- CVE-2022-27595 CVE-2022-27600

### Bilan de la vulnérabilité

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

### Solution

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

## Risques

- Déni de service
- Exécution de code arbitraire

## Référence

Bulletins de sécurité de QNAP :

- <https://www.qnap.com/fr-fr/security-advisory/qs-a-23-04>
- <https://www.qnap.com/fr-fr/security-advisory/qs-a-23-09>