



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités critiques affectant des produits QNAP
<b>Numéro de Référence</b>	41053003/23
<b>Date de Publication</b>	30 Mars 2023
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- QTS versions antérieures à 5.0.1.2346 build 20230322
- QuTS hero versions antérieures à h5.0.1.2348 build 20230324

### Identificateurs externes

CVE-2023-0286	CVE-2022-4304	CVE-2023-0215	CVE-2022-4450
CVE-2023-22809	CVE-2023-23355	CVE-2022-27597	CVE-2022-27598
CVE-2022-42898	CVE-2022-3437	CVE-2022-3592	

### 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, d'accéder à des informations confidentielles ou de contourner les mesures de sécurité.

### Solution

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

## Risques

- Exécution de code arbitraire
- Accès à des informations confidentielles
- Contournement des mesures de sécurité

## Références

Bulletins de sécurité de QNAP :

- <https://www.qnap.com/en/security-advisory/qa-23-15>
- <https://www.qnap.com/en/security-advisory/qa-23-11>
- <https://www.qnap.com/en/security-advisory/qa-23-10>
- <https://www.qnap.com/en/security-advisory/qa-23-06>
- <https://www.qnap.com/en/security-advisory/qa-23-03>
- <https://www.qnap.com/en/security-advisory/qa-23-02>