



## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités affectant des produits QNAP
<b>Numéro de Référence</b>	51370912/24
<b>Date de Publication</b>	09 Décembre 2024
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systemes affectés

- License Center versions 1.9.x antérieures à QTS 1.9.43
- QTS 5.1.x versions antérieures à QTS 5.1.9.2954 build 20241120
- QTS 5.2.x versions antérieures à QTS 5.2.2.2950 build 20241114
- QuTS hero h5.1.x versions antérieures à QuTS hero h5.1.9.2954 build 20241120
- QuTS hero h5.2.x versions antérieures à QuTS hero h5.2.2.2952 build 20241116

### Identificateurs externes

CVE-2024-48859 CVE-2024-48865 CVE-2024-48866 CVE-2024-48867 CVE-2024-48868  
CVE-2024-50393 CVE-2024-50402 CVE-2024-50403 CVE-2024-48863

### 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'injecter des commandes ou d'accéder à des données confidentielles.

### Solution

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

## Risques

- Exécution de commandes
- Accès à des données confidentielles

## Référence

Bulletins de sécurité de QNAP :

- <https://www.qnap.com/en/security-advisory/qs-a-24-50>
- <https://www.qnap.com/en/security-advisory/qs-a-24-49>