



.....  
Centre de Veille de Détection et de  
Réaction aux Attaques Informatiques

## BULLETIN DE SECURITE

<b>Titre</b>	Vulnérabilités affectant des produits QNAP
<b>Numéro de Référence</b>	61051202/26
<b>Date de Publication</b>	12 février 2026
<b>Risque</b>	Important
<b>Impact</b>	Important

### Systèmes affectés

- QTS 5.2.x
- QuTS hero h5.2.x
- QuTS hero h5.3.x

### Identificateurs externes

CVE-2024-42516 CVE-2024-43204 CVE-2024-43394 CVE-2024-47252 CVE-2025-9640  
CVE-2025-10230 CVE-2025-23048 CVE-2025-47205 CVE-2025-48725 CVE-2025-49630  
CVE-2025-49812 CVE-2025-53020 CVE-2025-54090 CVE-2025-58466 CVE-2025-59386  
CVE-2025-66274 CVE-2025-66277

### 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 d'exécuter du code à distance, d'accéder à des données confidentielles, de contourner des 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 à distance
- Accès à des données confidentielles
- Contournement de mesures de sécurité
- Dénier de service

## Référence

Bulletins de sécurité de QNAP :

- <https://www.qnap.com/en/security-advisory/qa-26-04>
- <https://www.qnap.com/en/security-advisory/qa-26-05>
- <https://www.qnap.com/en/security-advisory/qa-26-06>
- <https://www.qnap.com/en/security-advisory/qa-26-08>