ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Vulnérabilités critiques dans les produits QNAP
Numéro de Référence	58191011/25
Date de Publication	10 Novembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Hyper Data Protector 2.2.x versions antérieures 2.2.4.1
- QuMagie 2.6.x versions antérieures 2.7.0
- Download Station 5.10.x (pour QTS 5.2.1) versions antérieures 5.10.0.305
- Download Station 5.10.x (pour QuTS hero h5.2.1) versions antérieures 5.10.0.304
- File Station 5 version 5.5.x versions antérieures 5.5.6.5018
- Notification Center 1.9.x (pour QTS 5.2.x, QuTS hero h5.2.x) versions antérieures 1.9.2.3163
- Notification Center 2.1.x (pour QuTS hero h5.3.x) versions antérieures 2.1.0.3443
- Notification Center 3.0.x (pour QuTS hero h5.6.x, h6.0.x) versions antérieures 3.0.0.3466
- Qsync Central 5.0.x versions antérieures 5.0.0.3
- QuLog Center 1.8.x versions antérieures 1.8.2.923
- QuMagie 2.7.x versions antérieures 2.7.3
- Malware Remover 6.6.x versions antérieures 6.6.8.20251023
- QTS 5.2.x versions antérieures QTS 5.2.7.3297 build 20251024
- QuTS hero h5.2.x versions antérieures QuTS hero h5.2.7.3297 build 20251024
- QuTS hero h5.3.x versions antérieures QuTS hero h5.3.1.3292 build 20251024
- HBS 3 Hybrid Backup Sync 26.1.x et versions antérieures 26.2.0.938

Identificateurs externes

- CVE-2025-11837 CVE-2025-47207 CVE-2025-52425

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- CVE-2025-52865 CVE-2025-53408 CVE-2025-53409
- CVE-2025-53410 CVE-2025-53411 CVE-2025-53412
- CVE-2025-53413 CVE-2025-54167 CVE-2025-54168
- CVE-2025-57706 CVE-2025-57712 CVE-2025-58463
- CVE-2025-58464 CVE-2025-58465 CVE-2025-58469
- CVE-2025-62840 CVE-2025-62842 CVE-2025-62847
- CVE-2025-62848 CVE-2025-62849

Bilan de la vulnérabilité

QNAP a publié des mises à jour de sécurité critiques corrigeant sept vulnérabilités de type « zero-day » exploitées dans le cadre du concours Pwn2Own Ireland 2025 et plusieurs autres vulnérabilités.

L'exploitation de ces failles peut permettre à un attaquant non authentifié d'exécuter du code arbitraire et d'obtenir un contrôle complet sur les périphériques NAS vulnérables, de causer un déni de service, de réussir des injections SQL et de porter atteinte à la confidentialité des données.

Solution

Veuillez se référer au bulletin de sécurité Qnap du 08 Novembre 2025 pour plus d'information.

Risque

- Exécution du code arbitraire à distance
- Atteinte à la confidentialité des données
- Contournement de la politique de sécurité
- Déni de service à distance
- Exécution de code arbitraire à distance
- Injection SQL

Annexe

Bulletin de sécurité Septembre du 08 Novembre 2025:

- https://www.qnap.com/en/security-advisory/qsa-25-48
- https://www.qnap.com/en/security-advisory/qsa-25-33
- https://www.qnap.com/en/security-advisory/qsa-25-37
- https://www.qnap.com/en/security-advisory/qsa-25-38
- https://www.qnap.com/en/security-advisory/qsa-25-40
- https://www.qnap.com/en/security-advisory/qsa-25-41
- https://www.qnap.com/en/security-advisory/qsa-25-42
- https://www.qnap.com/en/security-advisory/qsa-25-43
- https://www.qnap.com/en/security-advisory/qsa-25-47
- https://www.qnap.com/en/security-advisory/qsa-25-45
- https://www.qnap.com/en/security-advisory/qsa-25-46