



Alerte Cyber : Failles de sécurité critiques dans les produits Qnap



Publié le 06 Mai 2024

Alerte cyber

faille de sécurité

qnap

vulnérabilité

Temps de lecture : 59 min

ALERTE
CYBERSÉCURITÉ



**Failles de sécurité critiques dans les
produits Qnap**

Risques

Espionnage, vol, voire destruction de vos données suite à la prise de contrôle à distance de vos équipements concernés.

Description

Des **failles de sécurité critiques** ont été corrigées dans plusieurs logiciels des serveurs de stockage en réseau (NAS) **Qnap**.

L'exploitation de ces vulnérabilités par une personne malveillante peut lui **permettre la prise de contrôle à distance des équipements concernés** et l'espionnage, le vol, voire la destruction, d'informations confidentielles.

Des cybercriminels pourraient très prochainement exploiter ces failles pour conduire des attaques massives contre les systèmes vulnérables.

Qnap a publié des mises à jour qui corrigent ces vulnérabilités et protègent de leur exploitation.

Systèmes concernés

- QTS 5.x, 4.5.x
- QuTS hero h5.x, h4.5.x
- **QuTSccloud c5.x**
- **myQNAPcloud 1.0.x**
- **myQNAPcloud Link 2.4.x**
- **Media Streaming Add-on 500.1.x**

Mesures à prendre

Mettre à jour au plus vite les équipements concernés avec les correctifs de sécurité mis à disposition par l'éditeur.

Procédure

Se référer aux bulletins de sécurité (en anglais) de l'éditeur pour obtenir les correctifs :

- <https://www.qnap.com/fr-fr/security-advisory/qlsa-24-09>
- <https://www.qnap.com/fr-fr/security-advisory/qlsa-24-14>
- <https://www.qnap.com/fr-fr/security-advisory/qlsa-24-15>

Besoin d'assistance ?

Vous pouvez trouver sur [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) des prestataires de proximité susceptibles de vous apporter leur soutien dans la mise en œuvre de ces mesures : [ici](#).

Références

- ANSSI / CERT-FR : <https://www.cert.ssi.gouv.fr/avis/CERTFR-2024-AVI-0354/>
- CVE-2024-32764
- CVE-2024-32766
- CVE-2024-21899
- CVE-2023-47222
- ...

Aller plus loin avec [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) :
Pourquoi et comment bien gérer ses mises à jour ?



Avez-vous trouvé cet article intéressant et utile ?



INSCRIVEZ-VOUS À LA NEWSLETTER

Tenez-vous informé(e) de l'actualité de la cybermalveillance et des nouvelles menaces

Entrez votre adresse email



OK



À PROPOS

Qui sommes-nous ?

Presse

DIVERS

Plan du site

Données personnelles

Mentions légales

NOUS SUIVRE



[GOUVERNEMENT.FR](#)

[LEGIFRANCE](#)

[ELYSEE.FR](#)

[FRANCE.FR](#)

[SERVICE PUBLIC](#)

[DATA.GOUV.FR](#)