



NCSC-2025-0403

Kwetsbaarheden verholpen in QNAP besturingssystemen

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 29-12-2025

TLP:WHITE

Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

QNAP heeft kwetsbaarheden verholpen in QTS en QuTS hero

Duiding

De kwetsbaarheden omvatten een kritieke fout in de verwerking van argumentafscidders, een NULL pointer dereference die kan leiden tot Denial-of-Service (DoS) aanvallen, een SQL-injectie die ongeautoriseerde code-executie mogelijk maakt, en een authenticatie-bypass die toegang tot beperkte bronnen verleent. Deze kwetsbaarheden kunnen door kwaadwillenden worden misbruikt om de integriteit en beschikbaarheid van de systemen in gevaar te brengen. Alle genoemde kwetsbaarheden zijn verholpen in specifieke versies van QTS en QuTS hero.

Oplossingen

QNAP heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://www.qnap.com/en/security-advisory/qs-a-25-45>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-62847	6.9 MEDIUM
➤ CVE-2025-62848	8.7 HIGH
➤ CVE-2025-62849	5.2 MEDIUM
➤ CVE-2025-59385	9.3 CRITICAL

CWE's

CWE	Beschrijving
➤ CWE-88	

Improper Neutralization of Argument Delimiters in a Command ('Argument Injection')

- [CWE-89](#) Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
- [CWE-290](#) Authentication Bypass by Spoofing
- [CWE-476](#) NULL Pointer Dereference

Getroffen producten

QNAP

QTS

Quts
Hero

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.