



NCSC-2024-0467

Kwetsbaarheden verholpen in QNAP besturingssystemen

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-12-2024

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 verschillende versies van hun besturingssystemen, waaronder QTS en QuTS hero.

Duiding

De kwetsbaarheden omvatten onjuiste authenticatie, problemen met certificaatvalidatie, onjuiste URL-codering, CRLF-injectie en command injection. Deze kwetsbaarheden stelden aanvallers in staat om ongeautoriseerde toegang te verkrijgen, systeemfunctionaliteit te verstoren, applicatiegegevens te wijzigen en zelfs willekeurige commando's uit te voeren op Network Attached Storage (NAS) apparaten.

Oplossingen

QNAP heeft specifieke latere versies van het besturingssysteem uitgebracht om deze kwetsbaarheden te verhelpen. Organisaties die gebruikmaken van de getroffen QNAP-producten wordt aangeraden om te updaten naar deze versies om hun systemen te beveiligen. Zie bijgevoegde referenties voor meer informatie.

Referenties

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

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2024-48859	
➤ CVE-2024-48865	
➤ CVE-2024-48866	
➤ CVE-2024-48867	
➤ CVE-2024-48868	
➤ CVE-2024-50393	
➤ CVE-2024-50402	
➤ CVE-2024-50403	

CWE's

CWE	Beschrijving
> CWE-177	Improper Handling of URL Encoding (Hex Encoding)
> CWE-93	Improper Neutralization of CRLF Sequences ('CRLF Injection')
> CWE-134	Use of Externally-Controlled Format String
> CWE-295	Improper Certificate Validation
> CWE-287	Improper Authentication

Getroffen producten

qnap
qts
quts_hero
qnap_systems_inc.
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.