Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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/qsa-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