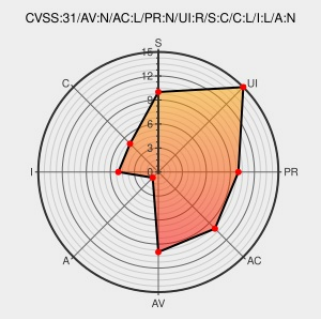
CVE-2020-2497

Published on: 12/09/2020 12:00:00 AM UTC

Last Modified on: 06/22/2021 09:00:00 PM UTC

CVE-2020-2497 - advisory for QSA-20-12

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Qts from Qnap contain the following vulnerability:

If exploited, this cross-site scripting vulnerability could allow remote attackers to inject malicious code in System Connection Logs. QANP have already fixed these vulnerabilities in the following versions of QTS and QuTS hero. QuTS hero h4.5.1.1472 build 20201031 and later QTS 4.5.1.1456 build 20201015 and later QTS 4.4.3.1354 build 20200702 and later QTS 4.3.6.1333 build 20200608 and later QTS 4.3.4.1368 build 20200703 and later QTS 4.3.3.1315 build 20200611 and later QTS 4.2.6 build 20200611 and later

CVE-2020-2497 has been assigned by security@qnap.com to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Multiple Vulnerabilities in QTS and QuTS hero - Security Advisory	Vendor Advisory	CONFIRM www.qnap.com/en/security

Multiple Vulnerabilities in QTS and QuTS hero - Security Advisory | QNAP	Vendor Advisory www.qnap.com text/html	CONFIRM www.qnap.com/en/security-advisory/qsa-20-12

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qnap	Qts	All	All	All	All
Operating System	Qnap	Qts	All	All	All	All
Application	Qnap	Qts	All	All	All	All
Application	Qnap	Quts Hero	All	All	All	All
Operating System	Qnap	Quts Hero	All	All	All	All
Application	Qnap	Quts Hero	All	All	All	All

cpe:2.3:a:qnap:qts:*:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:qts:*:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:*:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:quts_hero:*:*:*:*:*:*:*:*:

cpe:2.3:o:qnap:quts_hero:*:*:*:*:*:*:*:*:

cpe:2.3:a:qnap:quts_hero:*:*:*:*:*:*:*:*:

Discovery Credit

Jan Hoff

Social Mentions

Source	Title	Posted (UTC)

← Previous ID

Next ID→

© CVE.report 2023 | |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report