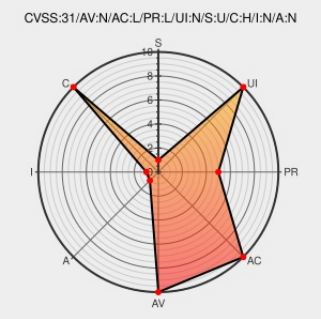
CVE-2021-44052

Published on: Not Yet Published

Last Modified on: 05/13/2022 08:18:00 PM UTC

CVE-2021-44052 - advisory for QSA-22-16

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



Certain versions of Qts from Qnap contain the following vulnerability:

An improper link resolution before file access ('Link Following') vulnerability has been reported to affect QNAP device running QuTScloud, QuTS hero, and QTS. If exploited, this vulnerability allows remote attackers to traverse the file system to unintended locations and read or overwrite the contents of unexpected files. We have already fixed this vulnerability in the following versions of QuTScloud, QuTS hero, and QTS: QuTScloud c5.0.1.1998 and later QuTS hero h4.5.4.1971 build 20220310 and later QuTS hero h5.0.0.1986 build 20220324 and later QTS 4.3.4.1976 build 20220303 and later QTS 4.3.3.1945 build 20220303 and later QTS 4.2.6 build 20220304 and later QTS 4.3.6.1965 build 20220302 and later QTS 5.0.0.1986 build 20220324 and later QTS 4.5.4.1991 build 20220329 and later

CVE-2021-44052 has been assigned by security@qnap.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.1 - HIGH

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

CVSS2 Score: 5.5 - MEDIUM

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

CVE References

Description	Tags	Link
Multiple Vulnerabilities in QTS, QuTS hero, and QuTScloud - Security Advisory | QNAP	www.qnap.com text/html	MISC www.qnap.com/en/security-advisory/qsa-22-16

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
Application	Qnap	Qts	4.2.6	build_20170517	All	All
Application	Qnap	Qts	4.2.6	build_20190322	All	All
Application	Qnap	Qts	4.2.6	build_20190730	All	All
Application	Qnap	Qts	4.2.6	build_20190921	All	All
Application	Qnap	Qts	4.2.6	build_20191107	All	All
Application	Qnap	Qts	4.2.6	build_20200109	All	All
Application	Qnap	Qts	4.2.6	build_20200421	All	All
Application	Qnap	Qts	4.2.6	build_20200611	All	All
Application	Qnap	Qts	4.2.6	build_20200821	All	All
Application	Qnap	Qts	4.2.6	build_20210327	All	All
Application	Qnap	Qts	4.2.6	build_20211215	All	All
Operating System	Qnap	Qutscloud	All	All	All	All
Operating System	Qnap	Quts Hero	All	All	All	All

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

cpe:2.3:a:qnap:qts:4.2.6:build_20170517:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.2.6:build_20190322:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.2.6:build_20190730:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.2.6:build_20190921:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.2.6:build_20191107:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.2.6:build_20200109:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.2.6:build_20200421:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.2.6:build_20200611:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.2.6:build_20200821:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.2.6:build_20210327:*:*:*:*:*:*:

cpe:2.3:a:qnap:qts:4.2.6:build_20211215:*:*:*:*:*:*:

cpe:2.3:o:qnap:qutscloud:*:*:*:*:*:*:*:*:

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

Discovery Credit

Enio Pena Navarro and Michael Messner from Siemens Energy AG

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-44052 : An improper link resolution before file access 'Link Following' vulnerability has been reported… twitter.com/i/web/status/1…	2022-05-05 16:56:49

← 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