



CVE-2018-19953

Published on: 10/28/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:39 PM UTC

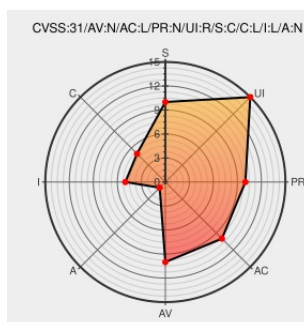
CVE-2018-19953

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. QNAP has already fixed the issue in the following QTS versions. QTS 4.4.2.1231 on build 20200302; QTS 4.4.1.1201 on build 20200130; QTS 4.3.6.1218 on build 20200214; QTS 4.3.4.1190 on build 20200107; QTS 4.3.3.1161 on build 20200109; QTS 4.2.6 on build 20200109.

CVE-2018-19953 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 File Station - Security Advisory QNAP	Vendor Advisory www.qnap.com text/html	MISC www.qnap.com/zh-tw/security-advisory/qa-20-01

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
Operating System	Qnap	Qts	All	All	All	All
Operating System	Qnap	Qts	4.2.6	-	All	All
Operating System	Qnap	Qts	4.2.6	build_20170517	All	All
Operating System	Qnap	Qts	4.2.6	build_20190322	All	All
Operating System	Qnap	Qts	4.2.6	build_20190730	All	All
Operating System	Qnap	Qts	4.2.6	build_20190921	All	All
Operating System	Qnap	Qts	4.2.6	build_20191107	All	All
Operating System	Qnap	Qts	All	All	All	All
Operating System	Qnap	Qts	4.2.6	-	All	All
Operating System	Qnap	Qts	4.2.6	build_20170517	All	All
Operating System	Qnap	Qts	4.2.6	build_20190322	All	All
Operating System	Qnap	Qts	4.2.6	build_20190730	All	All
Operating System	Qnap	Qts	4.2.6	build_20190921	All	All
Operating System	Qnap	Qts	4.2.6	build_20191107	All	All
cpe:2.3:o:qnap:qts:*****:						
cpe:2.3:o:qnap:qts:4.2.6:-:*****:						
cpe:2.3:o:qnap:qts:4.2.6:build_20170517:*****:						
cpe:2.3:o:qnap:qts:4.2.6:build_20190322:*****:						
cpe:2.3:o:qnap:qts:4.2.6:build_20190730:*****:						

cpe:2.3:o:qnap:qts:4.2.6:build_20190921:*****:
cpe:2.3:o:qnap:qts:4.2.6:build_20191107:*****:
cpe:2.3:o:qnap:qts:*****:
cpe:2.3:o:qnap:qts:4.2.6:-:*****:
cpe:2.3:o:qnap:qts:4.2.6:build_20170517:*****:
cpe:2.3:o:qnap:qts:4.2.6:build_20190322:*****:
cpe:2.3:o:qnap:qts:4.2.6:build_20190730:*****:
cpe:2.3:o:qnap:qts:4.2.6:build_20190921:*****:
cpe:2.3:o:qnap:qts:4.2.6:build_20191107:*****:

Discovery Credit

Independent Security Evaluators

[← 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 registered 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](#)