

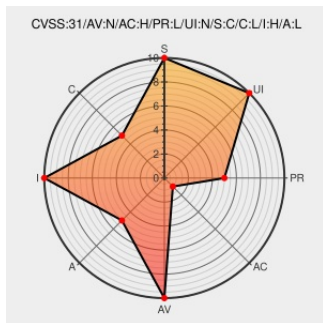


CVE-2018-0721

Published on: 11/27/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:50 PM UTC

CVE-2018-0721

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Qts](#) from [Qnap](#) contain the following vulnerability:

Buffer Overflow vulnerability in NAS devices. QTS allows attackers to run arbitrary code. This issue affects: QNAP Systems Inc. QTS version 4.2.6 and prior versions on build 20180711; version 4.3.3 and prior versions on build 20180725; version 4.3.4 and prior versions on build 20180710.

CVE-2018-0721 has been assigned by [Q security@qnap.com](#) to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [Q QNAP Systems Inc.](#) - QTS version <= 4.2.6

Affected Vendor/Software: [Q QNAP Systems Inc.](#) - QTS version <= 4.3.3

Affected Vendor/Software: [Q QNAP Systems Inc.](#) - QTS version <= 4.3.4

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **10 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description

Security Advisory for Vulnerabilities in QTS - Security Advisory | QNAP

Tags

Vendor Advisory

www.qnap.com

text/html

Link

CONFIRM www.qnap.com/zh-tw/security-advisory/nas-201809-20

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	4.2.6	All	All	All
Operating System	Qnap	Qts	4.3.3	All	All	All
Operating System	Qnap	Qts	4.3.4	All	All	All
Operating System	Qnap	Qts	4.2.6	All	All	All
Operating System	Qnap	Qts	4.3.3	All	All	All
Operating System	Qnap	Qts	4.3.4	All	All	All

cpe:2.3:o:qnap:qts:4.2.6:*****:

cpe:2.3:o:qnap:qts:4.3.3:*****:

cpe:2.3:o:qnap:qts:4.3.4:*****:

cpe:2.3:o:qnap:qts:4.2.6:*****:

cpe:2.3:o:qnap:qts:4.3.3:*****:

cpe:2.3:o:qnap:qts:4.3.4:*****:

Discovery Credit

Yuki, security researcher

← Previous ID

Next ID →

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](#)