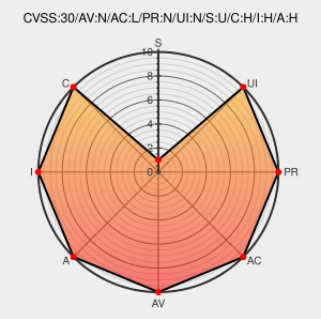
CVE-2018-0712

Published on: 06/21/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:48 PM UTC

CVE-2018-0712

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



Certain versions of Qts from Qnap contain the following vulnerability:

Command injection vulnerability in LDAP Server in QNAP QTS 4.2.6 build 20171208, QTS 4.3.3 build 20180402, QTS 4.3.4 build 20180413 and their earlier versions could allow remote attackers to run arbitrary commands or install malware on the NAS.

CVE-2018-0712 has been assigned by security@qnap.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **QNAP** - **LDAP Server in QTS** version **LDAP Server in QTS 4.2.6 build 20171208, QTS 4.3.3 build 20180402, QTS 4.3.4 build 20180413 and their earlier versions**

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: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Security Advisory for Command Injection Vulnerability in LDAP Server - Security Advisory | QNAP	Vendor Advisory www.qnap.com	CONFIRM www.qnap.com/zh-

	text/html	tw/security-advisory/nas-201806-19
QNAP QTS LDAP Server Command Injection Flaw Lets Remote Users Execute Arbitrary Commands on the Target System - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTRACK 1041141

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	4.2.6	All	All	All
Operating System	Qnap	Qts	4.3.3	All	All	All
Operating System	Qnap	Qts	All	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:4.2.6:*:*:*:*:*:*:*:

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

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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