



CVE-2017-17029

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2017-17029
State	PUBLISHED
Assigner	qnap
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-21 15:29:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	A buffer overflow vulnerability in login function in QNAP QTS version 4.2.6 build 20171026, 4.3.3.0378 build 20171117, 4.3

Risk And Classification

Primary CVSS: v3.0 9.8 CRITICAL from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.032360000 probability, percentile 0.872060000 (date 2026-05-13)

Problem Types: CWE-119 | Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	9.8	CRITICAL	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	7.5		AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Qnap	Qts	4.3.4.0358	beta1	All	All
Operating System	Qnap	Qts	4.3.4.0370	beta1	All	All
Operating System	Qnap	Qts	4.3.4.0372	beta1	All	All
Operating System	Qnap	Qts	4.3.4.0374	beta1	All	All
Operating System	Qnap	Qts	4.3.4.0387	beta2	All	All
Operating System	Qnap	Qts	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	QNAP	QTS Login Function	affected 4.2.6 build 20171026, 4.3.3.0378 build 20171117, 4.3.4.0387 (Beta 2) build 20171116 and

References

Reference	Source
Security Advisory for Buffer Overflow Vulnerabilities in QTS - Security Advisory QNAP	af854a3a-2127-422b-91ae-364da266
QNAP Storage Devices Buffer Overflow Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-364da266
CVE Program record	CVE.ORG

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)