



# QuRouter

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2025-62845
<b>State</b>	PUBLISHED
<b>Assigner</b>	qnap
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-20 17:16:42 UTC
<b>Updated</b>	2026-04-14 14:25:40 UTC
<b>Description</b>	An improper neutralization of escape, meta, or control sequences vulnerability has been reported to affect QHora. If a local

## Risk And Classification

**Primary CVSS:** v4.0 5.6 MEDIUM from security@qnapsecurity.com.tw

**CVSS:**4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:H/SI:H/SA:H/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

**EPSS:** 0.000160000 probability, percentile 0.033640000 (date 2026-04-15)

**Problem Types:** CWE-150 | CWE-150 CWE-150

Version	Source	Type	Score	Severity	Vector
4.0	security@qnapsecurity.com.tw	Secondary	5.6	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:H/SI:H/SA:H/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	5.6	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:H/SI:H/SA:H/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	nvd@nist.gov	Primary	6.7	MEDIUM	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

## CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

High

User Interaction

None

Confidentiality

Confidentiality

High

Integrity

Low

Availability

Low

Sub Conf.

High

Sub Integrity

High

Sub Availability

High

CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:H/SI:H/SA:H/E:U/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

### CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

High

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

### NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Qnap	Qurouter	2.6.0.239	build_20250625	All	All
Operating System	Qnap	Qurouter	2.6.0.688	build_20250818	All	All
Operating System	Qnap	Qurouter	2.6.1.028	build_20251001	All	All
Operating System	Qnap	Qurouter	2.6.2.007	build_20251027	All	All

### Vendor Declared Affected Products

#### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">QNAP Systems Inc.</a>	<a href="#">QuRouter</a>	affected 2.6.x 2.6.3.009 custom	Not specified

#### References

Reference	Source	Link	Tags
<a href="http://www.qnap.com/en/security-advisory/qlsa-26-12">www.qnap.com/en/security-advisory/qlsa-26-12</a>	<a href="mailto:security@qnapsecurity.com.tw">security@qnapsecurity.com.tw</a>	<a href="http://www.qnap.com">www.qnap.com</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

#### Vendor Comments And Credit

##### Discovery Credit

**CNA:** Pwn2Own 2025 - Team DDOS (en)

#### Additional Advisory Data

##### Solutions

**CNA:** We have already fixed the vulnerability in the following version: QuRouter 2.6.3.009 and later

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](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)