



QuRouter

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2025-62843 |
| State | PUBLISHED |
| Assigner | qnap |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2026-03-20 17:16:42 UTC |
| Updated | 2026-04-14 14:19:26 UTC |
| Description | An improper restriction of communication channel to intended endpoints vulnerability has been reported to affect QHora. If a |

Risk And Classification

Primary CVSS: v4.0 0.9 LOW from security@qnapsecurity.com.tw

CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:L/SA:N/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: 0.000240000 probability, percentile 0.063260000 (date 2026-04-15)

Problem Types: CWE-923 | CWE-923 CWE-923

| Version | Source | Type | Score | Severity | Vector |
|---------|------------------------------|-----------|-------|----------|--|
| 4.0 | security@qnapsecurity.com.tw | Secondary | 0.9 | LOW | CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:L |
| 4.0 | CNA | CVSS | 0.9 | LOW | CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:L |
| 3.1 | nvd@nist.gov | Primary | 6.8 | MEDIUM | CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H |

CVSS v4.0 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

Confidentiality

Confidentiality

None

Integrity

None

Availability

None

Sub Conf.

High

Sub Integrity

Low

Sub Availability

None

CVSS:4.0/AV:P/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:H/SI:L/SA:N/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

CVSS v3.1 Breakdown

Attack Vector

Physical

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:P/AC:L/PR:N/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 | QNAP Systems Inc. | QuRouter | affected 2.6.x 2.6.3.009 custom | Not specified |

References

| Reference | Source | Link | Tags |
|--|--|--|---------------------|
| www.qnap.com/en/security-advisory/qa-26-12 | security@qnapsecurity.com.tw | www.qnap.com | Vendor Advisory |
| CVE Program record | CVE.ORG | www.cve.org | canonical |
| NVD vulnerability detail | NVD | nvd.nist.gov | 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

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