

CVE-2020-2506

QNAP Systems QNAP Helpdesk Improper Access Control Vulnerability

CISA KEV since Mar 25, 2022

Actively exploited

The vulnerability have been reported to affect earlier versions of QTS. If exploited, this improper access control vulnerability could allow attackers to compromise the security of the software by gaining privileges, or reading sensitive information. This issue affects: QNAP Systems Inc. Helpdesk versions prior to 3.0.3.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.020 80.4th percentile · FIRST	CISA DEADLINE Apr 15, 2022 KEV since 2022 · listed over a year
--	---	---	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.020 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

Affected and fixed versions

PACKAGE	AFFECTED	FIXED IN	SOURCE
helpdesk	< 3.0.3	3.0.3	NVD

Sources

Vendor guidance github.com/advisories/GHSA-vph4-5mf4-28v5
NVD nvd.nist.gov/vuln/detail/CVE-2020-2506**Additional guidance** qnap.com/zh-tw/security-advisory/qa-20-08
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2020-22299**Current data** evulnable.com/vulnerability-management/cve/CVE-2020-2506

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.