

CVE-2018-19949

QNAP NAS File Station Command Injection Vulnerability

Exigent

CISA KEV since May 24, 2022

Actively exploited

Ransomware use known

If exploited, this command injection vulnerability could allow remote attackers to run arbitrary commands. QNAP has already fixed the issue in the following QTS versions. QTS 4.4.2.1231 on build 20200302; QTS 4.4.1.1201 on build 20200130; QTS 4.3.6.1218 on build 20200214; QTS 4.3.4.1190 on build 20200107; QTS 4.3.3.1161 on build 20200109; QTS 4.2.6 on build 20200109.

EVRS 85/100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.302 98.2nd percentile · FIRST	CISA DEADLINE Jun 14, 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.302 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent 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
qts	< 4.2.6 ≥ 4.3.1.0013 < 4.3.3.1161 ≥ 4.3.4 < 4.3.4.1190 ≥ 4.3.6 < 4.3.6.1218 ≥ 4.4.0 < 4.4.1.1201 ≥ 4.4.2 < 4.4.2.1231 4.2.6	4.2.6 · 4.3.3.1161 · 4.3.4.1190 · 4.3.6.1218 · 4.4.1.1201 · 4.4.2.1231	NVD

Sources

Vendor guidance github.com/advisories/GHSA-h9cw-v634-8jcw
NVD nvd.nist.gov/vuln/detail/CVE-2018-19949

Additional guidance qnap.com/zh-tw/security-advisory/qa-20-01
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2018-11620

Current data evulnable.com/vulnerability-management/cve/CVE-2018-19949

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