

CVE-2020-2509

QNAP Network-Attached Storage (NAS) Command Injection Vulnerability

CISA KEV since Apr 11, 2022

Actively exploited

A command injection vulnerability has been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. We have already fixed this vulnerability in the following versions: QTS 4.5.2.1566 Build 20210202 and later QTS 4.5.1.1495 Build 20201123 and later QTS 4.3.6.1620 Build 20210322 and later QTS 4.3.4.1632 Build 20210324 and later QTS 4.3.3.1624 Build 20210416 and later QTS 4.2.6 Build 20210327 and later QuTS hero h4.5.1.1491 build 20201119 and later

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.340 98.4th percentile · FIRST	CISA DEADLINE May 2, 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	0.340 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

qts	< 4.2.6	4.2.6 · 4.3.6 · 4.5.1	NVD
	≥ 4.3.5 < 4.3.6		
	≥ 4.4.0 < 4.5.1		
	4.2.6		
	4.3.3.0174		
	4.3.3.0868		
	4.3.3.0998		
	4.3.3.1051		
	4.3.3.1098		
	4.3.3.1161		
	4.3.3.1252		
	4.3.3.1315		
	4.3.3.1386		
	4.3.3.1432		
	4.3.4.0358		
	4.3.4.0370		
	4.3.4.0372		
	4.3.4.0374		
	4.3.4.0387		
	4.3.4.0411		
	4.3.4.0416		
	4.3.4.0427		
	4.3.4.0434		
	4.3.4.0435		
	4.3.4.0451		
	4.3.4.0483		
	4.3.4.0486		
	4.3.4.0506		
	4.3.4.0516		
	4.3.4.0526		
	4.3.4.0551		
	4.3.4.0557		
	4.3.4.0561		
	4.3.4.0569		
	4.3.4.0593		
	4.3.4.0597		
	4.3.4.0604		
	4.3.4.0899		
	4.3.4.1029		
	4.3.4.1082		
	4.3.4.1190		
	4.3.4.1282		
	4.3.4.1368		
	4.3.4.1417		
	4.3.4.1463		
	4.3.6		
	4.3.6.0895		
	4.3.6.0907		
	4.3.6.0923		
	4.3.6.0944		
	4.3.6.0959		
	4.3.6.0979		
	4.3.6.0993		
	4.3.6.1013		
	4.3.6.1033		
	4.3.6.1070		
	4.3.6.1154		
	4.3.6.1218		
	4.3.6.1263		
	4.3.6.1286		
	4.3.6.1333		
	4.3.6.1411		
	4.3.6.1446		



PACKAGE	AFFECTED	FIXED IN	SOURCE
	4.5.1 4.5.1.1456 4.5.1.1461 4.5.1.1465 4.5.1.1480 4.5.2		
quts hero	< h4.5.1 h4.5.1 h4.5.1.1472	h4.5.1	NVD

Sources

Vendor guidance github.com/advisories/GHSA-77jf-5mcg-g6m9
NVD nvd.nist.gov/vuln/detail/CVE-2020-2509

Additional guidance qnap.com/en/security-advisory/qa-21-05
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2020-2509

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-22302

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