

CVE-2019-7195

QNAP Photo Station Path Traversal Vulnerability

Exigent
CISA KEV since Jun 8, 2022
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

This external control of file name or path vulnerability allows remote attackers to access or modify system files. To fix the vulnerability, QNAP recommend updating Photo Station to their latest versions.

EVRS 91 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.897 99.79th percentile · FIRST	CISA DEADLINE Jun 22, 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	0.897 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
photo station	< 6.0.3 < 5.7.10 < 5.4.9 < 5.2.11	6.0.3 · 5.7.10 · 5.4.9 · 5.2.11	NVD
qts	4.4.1 ≥ 4.3.4 ≤ 4.4.0 ≥ 4.3.0 ≤ 4.3.3 4.2.6	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-5h7g-3542-fw4q	Additional guidance	qnap.com/zh-tw/security-advisory/nas-201911-25
NVD	nvd.nist.gov/vuln/detail/CVE-2019-7195	CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog
ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2019-16739	Current data	evulnable.com/vulnerability-management/cve/CVE-2019-7195

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