



CVE-2019-7194

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

Summary

CVE	CVE-2019-7194
State	PUBLIC
Assigner	security@qnap.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-05 17:15:00 UTC
Updated	2022-04-22 19:59:00 UTC
Description	This external control of file name or path vulnerability allows remote attackers to access or modify system files. To fix the v

Risk And Classification

EPSS: 0.939380000 probability, percentile 0.998790000 (date 2026-04-01)

CISA KEV: Listed on 2022-06-08; due 2022-06-22; ransomware use Known

Problem Types: CWE-22

CISA Known Exploited Vulnerability

Vendor	QNAP
Product	Photo Station
Name	QNAP Photo Station Path Traversal Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2019-7194

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Qnap	Photo Station	All	All	All	All
Application	Qnap	Photo Station	All	All	All	All
Operating System	Qnap	Qts	4.2.6	All	All	All
Operating System	Qnap	Qts	4.4.1	All	All	All
Operating System	Qnap	Qts	All	All	All	All
Operating System	Qnap	Qts	All	All	All	All
Operating System	Qnap	Qts	4.2.6	All	All	All
Operating System	Qnap	Qts	4.4.1	All	All	All

Operating System	Qnap	Qts	All	All	All	All
Operating System	Qnap	Qts	All	All	All	All

References

Reference	Source	Link	Tags
Security Advisory for Vulnerabilities in QTS and Photo Station - Technical Advisory QNAP	CONFIRM	www.qnap.com	Vendo
QNAP QTS And Photo Station 6.0.3 Remote Command Execution ≈ Packet Storm	MISC	packetstormsecurity.com	
CVE Program record	CVE.ORG	www.cve.org	canoni
NVD vulnerability detail	NVD	nvd.nist.gov	canoni
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.gov	kev

No vendor comments have been submitted for this CVE.

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](#).

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