



CVE-2013-7174

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

Summary

CVE	CVE-2013-7174
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-09 18:07:00 UTC
Updated	2016-12-31 02:59:00 UTC
Description	Absolute path traversal vulnerability in cgi-bin/jc.cgi in QNAP QTS before 4.1.0 allows remote attackers to read arbitrary file

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Qnap	Qts	4.0	All	All	All
Operating System	Qnap	Qts	4.0	All	All	All
Operating System	Qnap	Qts	All	All	All	All

References

Reference	Source	Link	Tags
QNAP QTS Input Validation Flaw in 'jc.cgi' Lets Remote Users View Files - SecurityTracker	SECTrack	www.securitytracker.com	
QNAP QTS 'f' Parameter Directory Traversal Vulnerability	BID	www.securityfocus.com	
Vulnerability Note VU#487078 - QNAP QTS path traversal vulnerability	CERT-VN	www.kb.cert.org	US C
CVE Program record	CVE.ORG	www.cve.org	cano
NVD vulnerability detail	NVD	nvd.nist.gov	cano

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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)