CVE-2013-4131

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2013-4131
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-07-31 13:20:28 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The mod_dav_svn Apache HTTPD server module in Subversion 1.7.0 through 1.7.10 and 1.8.x before 1.8.1 allows remote

Risk And Classification

Primary CVSS: v2.0 4 from nvd@nist.gov

AV:N/AC:L/Au:S/C:N/I:N/A:P

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:L/Au:S/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Subversion	1.7.0	All	All	All

Application	Apache	Subversion	1.7.1	All	All	All
Application	Apache	Subversion	1.7.10	All	All	All
Application	Apache	Subversion	1.7.2	All	All	All
Application	Apache	Subversion	1.7.3	All	All	All
Application	Apache	Subversion	1.7.4	All	All	All
Application	Apache	Subversion	1.7.5	All	All	All
Application	Apache	Subversion	1.7.6	All	All	All
Application	Apache	Subversion	1.7.7	All	All	All
Application	Apache	Subversion	1.7.8	All	All	All
Application	Apache	Subversion	1.7.9	All	All	All
Application	Apache	Subversion	1.8.0	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
subversion.apache.org/security/CVE-2013-4131-advisory.txt
Apache Subversion CVE-2013-4131 Denial Of Service Vulnerability
openSUSE-SU-2013:1286-1: moderate: subversion: update to 1.7.11
Repository / Oval Repository
986194 – (CVE-2013-4131) CVE-2013-4131 subversion: DoS (assertion failure, crash) in mod_dav_svn when handling certain MOVE, COPY
IBM X-Force Exchange
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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