



CVE-2013-6892

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

Summary

CVE	CVE-2013-6892
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-21 18:59:00 UTC
Updated	2016-08-26 19:25:00 UTC
Description	WebSVN 2.3.3 allows remote authenticated users to read arbitrary files via a symlink attack in a commit.

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Websvn	Websvn	2.3.3	All	All	All
Application	Websvn	Websvn	2.3.3	All	All	All

References

Reference	Source
#775682 - websvn: CVE-2013-6892: arbitrary file access when downloads enabled for users with commit access - Debian Bug report logs	MITRE
Security Advisory SA62233 - WebSVN Symlink Arbitrary File Download Vulnerability - Secunia	Secunia
Debian -- Security Information -- DSA-3137-1 websvn	Debian
CVE Program record	CVE Program
NVD vulnerability detail	NVD

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](#)