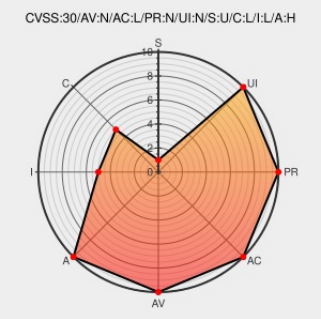
CVE-2015-5259

Published on: 01/08/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

CVE-2015-5259

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Subversion from Apache contain the following vulnerability:

Integer overflow in the read_string function in libsvn_ra_svn/marshal.c in Apache Subversion 1.9.x before 1.9.3 allows remote attackers to execute arbitrary code via an svn:// protocol string, which triggers a heap-based buffer overflow and an out-of-bounds read.

CVE-2015-5259 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.6 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	LOW	LOW	HIGH

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	COMPLETE

CVE References

Description	Tags	Link
	Vendor Advisory, subversion.apache.org, text/x-diff	CONFIRM subversion.apache.org/security/CVE-2015-5259-advisory.txt
Apache Subversion CVE-2015-5259 Integer Overflow Vulnerability	cve.report (archive)	BID 82300

	text/html	
Apache Subversion Heap Overflow Lets Remote Users Deny Service and Potentially Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034469
Subversion, Serf: Multiple Vulnerabilities (GLSA 201610-05) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201610-05

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Subversion	1.9.0	All	All	All
Application	Apache	Subversion	1.9.1	All	All	All
Application	Apache	Subversion	1.9.2	All	All	All
Application	Apache	Subversion	1.9.0	All	All	All
Application	Apache	Subversion	1.9.1	All	All	All
Application	Apache	Subversion	1.9.2	All	All	All

cpe:2.3:a:apache:subversion:1.9.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:subversion:1.9.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:subversion:1.9.2:*:*:*:*:*:*:*:

cpe:2.3:a:apache:subversion:1.9.0:*:*:*:*:*:*:*:

cpe:2.3:a:apache:subversion:1.9.1:*:*:*:*:*:*:*:

cpe:2.3:a:apache:subversion:1.9.2:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→