



CVE-2017-9800

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

Summary

CVE	CVE-2017-9800
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-11 21:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	A maliciously constructed svn+ssh:// URL would cause Subversion clients before 1.8.19, 1.9.x before 1.9.7, and 1.10.0.x th

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Subversion	1.10.0	All	All	All
Application	Apache	Subversion	1.10.0	alpha1	All	All
Application	Apache	Subversion	1.10.0	alpha2	All	All
Application	Apache	Subversion	1.10.0	alpha3	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
Application	Apache	Subversion	1.9.3	All	All	All
Application	Apache	Subversion	1.9.4	All	All	All
Application	Apache	Subversion	1.9.5	All	All	All
Application	Apache	Subversion	1.9.6	All	All	All
Application	Apache	Subversion	1.10.0	All	All	All
Application	Apache	Subversion	1.10.0	alpha1	All	All
Application	Apache	Subversion	1.10.0	alpha2	All	All
Application	Apache	Subversion	1.10.0	alpha3	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
Application	Apache	Subversion	1.9.3	All	All	All
Application	Apache	Subversion	1.9.4	All	All	All
Application	Apache	Subversion	1.9.5	All	All	All
Application	Apache	Subversion	1.9.6	All	All	All
Application	Apache	Subversion	All	All	All	All

References

Reference

Pony Mail!

[Apache Subversion CVE-2017-9800 Remote Command Execution Vulnerability](#)

[SourceTree Security Advisory 2017-08-11 - Atlassian Documentation](#)

Pony Mail!

[Apache Subversion Arbitrary Code Execution ≈ Packet Storm](#)

[SecurityFocus](#)

[Oracle Critical Patch Update Advisory - October 2020](#)

[Apache Subversion 'svn+ssh://' URL Processing Flaw Lets Remote Users Execute Arbitrary Commands on the Target System - SecurityTrack](#)

Pony Mail!

[About the security content of Xcode 9 - Apple Support](#)

[Red Hat Customer Portal](#)

[Subversion: Arbitrary code execution \(GLSA 201709-09\) — Gentoo security](#)

[Debian -- Security Information -- DSA-3932-1 subversion](#)

[subversion.apache.org/security/CVE-2017-9800-advisory.txt](#)

Pony Mail!

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500673](#) Alpine Linux Security Update for subversion

[504447](#) Alpine Linux Security Update for subversion

[690554](#) Free Berkeley Software Distribution (FreeBSD) Security Update for subversion (6e80bd9b-7e9b-11e7-abfe-90e2baa3bafc)

[710440](#) Gentoo Linux Subversion Arbitrary code execution Vulnerability (GLSA 201709-09)

© [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](#)