



CVE-2017-1000117

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

Summary

CVE	CVE-2017-1000117
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-05 01:29:00 UTC
Updated	2023-11-07 02:37:00 UTC
Description	A malicious third-party can give a crafted "ssh://..." URL to an unsuspecting victim, and an attempt to visit the URL can result in a remote code execution (RCE) on the victim's system.

Risk And Classification

Problem Types: CWE-601

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Git-scm	Git	2.10.0	All	All	All
Application	Git-scm	Git	2.10.0	rc0	All	All
Application	Git-scm	Git	2.10.0	rc1	All	All
Application	Git-scm	Git	2.10.0	rc2	All	All
Application	Git-scm	Git	2.10.1	All	All	All
Application	Git-scm	Git	2.10.2	All	All	All
Application	Git-scm	Git	2.10.3	All	All	All
Application	Git-scm	Git	2.11.0	All	All	All
Application	Git-scm	Git	2.11.0	rc0	All	All
Application	Git-scm	Git	2.11.0	rc1	All	All
Application	Git-scm	Git	2.11.0	rc2	All	All
Application	Git-scm	Git	2.11.0	rc3	All	All
Application	Git-scm	Git	2.11.1	All	All	All
Application	Git-scm	Git	2.11.2	All	All	All
Application	Git-scm	Git	2.12.0	All	All	All
Application	Git-scm	Git	2.12.0	rc0	All	All
Application	Git-scm	Git	2.12.0	rc1	All	All

Application	Git-scm	Git	2.12.0	rc2	All	All
Application	Git-scm	Git	2.12.1	All	All	All
Application	Git-scm	Git	2.12.2	All	All	All
Application	Git-scm	Git	2.12.3	All	All	All
Application	Git-scm	Git	2.13.0	All	All	All
Application	Git-scm	Git	2.13.0	rc0	All	All
Application	Git-scm	Git	2.13.0	rc1	All	All
Application	Git-scm	Git	2.13.0	rc2	All	All
Application	Git-scm	Git	2.13.1	All	All	All
Application	Git-scm	Git	2.13.2	All	All	All
Application	Git-scm	Git	2.13.3	All	All	All
Application	Git-scm	Git	2.13.4	All	All	All
Application	Git-scm	Git	2.14.0	All	All	All
Application	Git-scm	Git	2.14.0	rc0	All	All
Application	Git-scm	Git	2.14.0	rc1	All	All
Application	Git-scm	Git	2.8.0	All	All	All
Application	Git-scm	Git	2.8.0	rc0	All	All
Application	Git-scm	Git	2.8.0	rc1	All	All
Application	Git-scm	Git	2.8.0	rc2	All	All
Application	Git-scm	Git	2.8.0	rc3	All	All
Application	Git-scm	Git	2.8.1	All	All	All
Application	Git-scm	Git	2.8.2	All	All	All
Application	Git-scm	Git	2.8.3	All	All	All
Application	Git-scm	Git	2.8.4	All	All	All
Application	Git-scm	Git	2.8.5	All	All	All
Application	Git-scm	Git	2.9.0	All	All	All
Application	Git-scm	Git	2.9.0	rc0	All	All
Application	Git-scm	Git	2.9.0	rc1	All	All
Application	Git-scm	Git	2.9.0	rc2	All	All
Application	Git-scm	Git	2.9.1	All	All	All
Application	Git-scm	Git	2.9.2	All	All	All
Application	Git-scm	Git	2.9.3	All	All	All
Application	Git-scm	Git	2.9.4	All	All	All
Application	Git-scm	Git	2.10.0	All	All	All
Application	Git-scm	Git	2.10.0	rc0	All	All

Application	Git-scm	Git	2.10.0	rc1	All	All
Application	Git-scm	Git	2.10.0	rc2	All	All
Application	Git-scm	Git	2.10.1	All	All	All
Application	Git-scm	Git	2.10.2	All	All	All
Application	Git-scm	Git	2.10.3	All	All	All
Application	Git-scm	Git	2.11.0	All	All	All
Application	Git-scm	Git	2.11.0	rc0	All	All
Application	Git-scm	Git	2.11.0	rc1	All	All
Application	Git-scm	Git	2.11.0	rc2	All	All
Application	Git-scm	Git	2.11.0	rc3	All	All
Application	Git-scm	Git	2.11.1	All	All	All
Application	Git-scm	Git	2.11.2	All	All	All
Application	Git-scm	Git	2.12.0	All	All	All
Application	Git-scm	Git	2.12.0	rc0	All	All
Application	Git-scm	Git	2.12.0	rc1	All	All
Application	Git-scm	Git	2.12.0	rc2	All	All
Application	Git-scm	Git	2.12.1	All	All	All
Application	Git-scm	Git	2.12.2	All	All	All
Application	Git-scm	Git	2.12.3	All	All	All
Application	Git-scm	Git	2.13.0	All	All	All
Application	Git-scm	Git	2.13.0	rc0	All	All
Application	Git-scm	Git	2.13.0	rc1	All	All
Application	Git-scm	Git	2.13.0	rc2	All	All
Application	Git-scm	Git	2.13.1	All	All	All
Application	Git-scm	Git	2.13.2	All	All	All
Application	Git-scm	Git	2.13.3	All	All	All
Application	Git-scm	Git	2.13.4	All	All	All
Application	Git-scm	Git	2.14.0	All	All	All
Application	Git-scm	Git	2.14.0	rc0	All	All
Application	Git-scm	Git	2.14.0	rc1	All	All
Application	Git-scm	Git	2.8.0	All	All	All
Application	Git-scm	Git	2.8.0	rc0	All	All
Application	Git-scm	Git	2.8.0	rc1	All	All
Application	Git-scm	Git	2.8.0	rc2	All	All
Application	Git-scm	Git	2.8.0	rc3	All	All

Application	Git-scm	Git	2.8.1	All	All	All
Application	Git-scm	Git	2.8.2	All	All	All
Application	Git-scm	Git	2.8.3	All	All	All
Application	Git-scm	Git	2.8.4	All	All	All
Application	Git-scm	Git	2.8.5	All	All	All
Application	Git-scm	Git	2.9.0	All	All	All
Application	Git-scm	Git	2.9.0	rc0	All	All
Application	Git-scm	Git	2.9.0	rc1	All	All
Application	Git-scm	Git	2.9.0	rc2	All	All
Application	Git-scm	Git	2.9.1	All	All	All
Application	Git-scm	Git	2.9.2	All	All	All
Application	Git-scm	Git	2.9.3	All	All	All
Application	Git-scm	Git	2.9.4	All	All	All
Application	Git-scm	Git	All	All	All	All

References

Reference	Source
[ANNOUNCE] Git v2.14.1, v2.13.5, and others	MISC
[ANNOUNCE] Git v2.14.1, v2.13.5, and others	
Red Hat Customer Portal	REDHAT
Red Hat Customer Portal	REDHAT
About the security content of Xcode 9 - Apple Support	CONFIRM
Red Hat Customer Portal	REDHAT
Git: Command injection (GLSA 201709-10) — Gentoo Security	GENTOO
Git 'ssh://' URL Processing Flaw Lets Remote Users Execute Arbitrary Commands on the Target System - SecurityTracker	SECTRACK
Red Hat Customer Portal	REDHAT
Git CVE-2017-1000117 Remote Command Injection Vulnerability	BID
Debian -- Security Information -- DSA-3934-1 git	DEBIAN
Red Hat Customer Portal	REDHAT
Git < 2.7.5 - Command Injection (Metasploit)	EXPLOIT-DB
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[378269](#) Virtuozzo Linux Security Update for git-cvs (VZLSA-2017:2485)

[500216](#) Alpine Linux Security Update for git

[503960](#) Alpine Linux Security Update for git

© [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](#)