



CVE-2015-7545

Published on: 04/13/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:12 PM UTC

CVE-2015-7545

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

The (1) git-remote-ext and (2) unspecified other remote helper programs in Git before 2.3.10, 2.4.x before 2.4.10, 2.5.x before 2.5.4, and 2.6.x before 2.6.1 do not properly restrict the allowed protocols, which might allow remote attackers to execute arbitrary code via a URL in a (a) .gitmodules file or (b) unknown other sources in a submodule.

CVE-2015-7545 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

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

CVSS2 Score: **7.5 - HIGH**

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

CVE References

Description	Tags	Link
Oracle Solaris Bulletin - April 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bul
GIT git-remote-ext Helper URI Processing Lets	www.securitytracker.com	SECTRACK 1034501

git: git remote ext helper CVE: Processing Local Remote Users Execute Arbitrary Commands on the Target System - SecurityTracker	www.securitytracker.com text/html	SECURITYTRACKER 1047001
git/2.4.10.txt at master · git/git · GitHub	Patch Vendor Advisory github.com text/html	CONFIRM github.com/git/git/blob/master/Documentation/Re
USN-2835-1: Git vulnerability Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2835-1
git/2.5.4.txt at master · git/git · GitHub	Patch Vendor Advisory github.com text/html	CONFIRM github.com/git/git/blob/master/Documentation/Re
LKML: Junio C Hamano: [ANNOUNCE] Git v2.6.1, v2.5.4, v2.4.10 and v2.3.10	lkml.org text/xml	MLIST [linux-kernel] 20151005 [ANNOUNCE] Git v2.6.1, v2
33cfccbbf35a56e190b79bdec5c85457c952a021 - pub/scm/git/git - Git at Google	kernel.googlesource.com text/html	CONFIRM kernel.googlesource.com/pub/scm/git/git/+/-/33cfccbbf35a56e19
git/2.6.1.txt at master · git/git · GitHub	github.com text/html	CONFIRM github.com/git/git/blob/master/Documentation/Re
The Slackware Linux Project: Slackware Security Advisories	www.slackware.com text/html	SLACKWARE SSA:2016-123-01
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:2515
Git CVE-2015-7545 Remote Command Execution Vulnerability	cve.report (archive) text/html	BID 78711
oss-security - Re: CVE for git issue - please use CVE-2015-7545	www.openwall.com text/html	MLIST [oss-security] 20151209 Re: CVE for git issue - plea
git/2.3.10.txt at master · git/git · GitHub	Patch Vendor Advisory github.com text/html	CONFIRM github.com/git/git/blob/master/Documentation/Re
oss-security - CVE for git issue - please use CVE-2015-7545	www.openwall.com text/html	MLIST [oss-security] 20151208 CVE for git issue - please u
1269794 – (CVE-2015-7545) CVE-2015-7545 git: arbitrary code execution via crafted URLs	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=1269794
Oracle Linux Bulletin - October 2015	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/linu 2719645.html
Oracle Linux Bulletin - January 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/linu 2867209.html
oss-security - Re: CVE for git issue - please use CVE-2015-7545	www.openwall.com text/html	MLIST [oss-security] 20151211 Re: CVE for git issue - plea
Debian -- Security Information -- DSA-3435-1 git	www.debian.org Deprecated Link text/html	DEBIAN DSA-3435
openSUSE-SU-2015:1968-1: moderate: Security update for git	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:1968
Git: Multiple vulnerabilities (GLSA 201605-01) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201605-01

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

Exploit/POC from Github

CVE-2015-7545 proof of concept

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Application	Git Project	Git	2.4.0	All	All	All
Application	Git Project	Git	2.4.1	All	All	All
Application	Git Project	Git	2.4.2	All	All	All
Application	Git Project	Git	2.4.3	All	All	All
Application	Git Project	Git	2.4.4	All	All	All
Application	Git Project	Git	2.4.5	All	All	All
Application	Git Project	Git	2.4.6	All	All	All
Application	Git Project	Git	2.4.7	All	All	All
Application	Git Project	Git	2.4.8	All	All	All
Application	Git Project	Git	2.4.9	All	All	All
Application	Git Project	Git	2.5.0	All	All	All
Application	Git Project	Git	2.5.1	All	All	All

Application	Git Project	Git	2.5.2	All	All	All
Application	Git Project	Git	2.5.3	All	All	All
Application	Git Project	Git	2.6.0	All	All	All
Application	Git Project	Git	2.4.0	All	All	All
Application	Git Project	Git	2.4.1	All	All	All
Application	Git Project	Git	2.4.2	All	All	All
Application	Git Project	Git	2.4.3	All	All	All
Application	Git Project	Git	2.4.4	All	All	All
Application	Git Project	Git	2.4.5	All	All	All
Application	Git Project	Git	2.4.6	All	All	All
Application	Git Project	Git	2.4.7	All	All	All
Application	Git Project	Git	2.4.8	All	All	All
Application	Git Project	Git	2.4.9	All	All	All
Application	Git Project	Git	2.5.0	All	All	All
Application	Git Project	Git	2.5.1	All	All	All
Application	Git Project	Git	2.5.2	All	All	All
Application	Git Project	Git	2.5.3	All	All	All
Application	Git Project	Git	2.6.0	All	All	All
Application	Git Project	Git	All	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Redhat	Software Collections	1.0	All	All	All
Application	Redhat	Software Collections	1.0	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:its:***:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:its:***:						
cpe:2.3:o:canonical:ubuntu_linux:15.04:*****:***:						
cpe:2.3:o:canonical:ubuntu_linux:15.10:*****:***:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:***:its:***:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:***:its:***:						

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:
cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.0:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.1:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.2:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.3:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.4:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.5:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.6:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.7:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.8:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.9:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.5.0:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.5.1:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.5.2:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.5.3:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.6.0:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.0:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.1:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.2:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.3:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.4:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.5:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.6:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.7:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.8:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.4.9:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.5.0:*:*:*:*:*:
cpe:2.3:a:git_project:git:2.5.1:*:*:*:*:*:

cpe:2.3:a:git_project:git:2.5.2:*****:
cpe:2.3:a:git_project:git:2.5.3:*****:
cpe:2.3:a:git_project:git:2.6.0:*****:
cpe:2.3:a:git_project:git:*****:
cpe:2.3:o:opensuse:opensuse:13.1:*****:
cpe:2.3:o:opensuse:opensuse:13.2:*****:
cpe:2.3:o:opensuse:opensuse:13.1:*****:
cpe:2.3:o:opensuse:opensuse:13.2:*****:
cpe:2.3:a:redhat:software_collections:1.0:*****:
cpe:2.3:a:redhat:software_collections:1.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)