



CVE-2018-17456

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

| | |
|------------------------|--|
| CVE | CVE-2018-17456 |
| State | PUBLIC |
| Assigner | cve@mitre.org |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2018-10-06 14:29:00 UTC |
| Updated | 2020-08-24 17:37:00 UTC |
| Description | Git before 2.14.5, 2.15.x before 2.15.3, 2.16.x before 2.16.5, 2.17.x before 2.17.2, 2.18.x before 2.18.1, and 2.19.x before 2 |

Risk And Classification

Problem Types: CWE-88

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|------------------|---------------------------|----------------------------------|---------|--------|---------|----------|
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 14.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 16.04 | All | All | All |
| Operating System | Canonical | Ubuntu Linux | 18.04 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Operating System | Debian | Debian Linux | 9.0 | All | All | All |
| Application | Git-scm | Git | All | All | All | All |
| Application | Git-scm | Git | All | All | All | All |
| Application | Redhat | Ansible Tower | 3.3 | All | All | All |
| Application | Redhat | Ansible Tower | 3.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 6.7 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.4 | All | All | All |

| | | | | | | |
|------------------|--------|------------------------------|-----|-----|-----|-----|
| Operating System | Redhat | Enterprise Linux | 7.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 6.7 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Aus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |

References

| Reference | Source | Link |
|--|------------|---|
| Git Submodule - Arbitrary Code Execution (PoC) - Linux local Exploit | EXPLOIT-DB | www.exploit-c |
| Red Hat Customer Portal | REDHAT | access.redha |
| Git Submodule - Arbitrary Code Execution - Linux local Exploit | EXPLOIT-DB | www.exploit-c |
| Sourcetreer Git Arbitrary Code Execution / URL Handling ≈ Packet Storm | MISC | packetstorms |
| Atlassian SourceTree CVE-2018-17456 Arbitrary Code Execution Vulnerability | BID | www.security |
| Red Hat Customer Portal | REDHAT | access.redha |
| Red Hat Customer Portal | REDHAT | access.redha |
| Debian -- Security Information -- DSA-4311-1 git | DEBIAN | www.debian.c |
| [security-announce] openSUSE-SU-2020:0598-1: moderate: Security update f | SUSE | lists.opensuse |
| '[Announce] Git 2.14.5, 2.15.3, 2.16.5, 2.17.2, 2.18.1, and 2.19.1' - MARC | MISC | marc.info |
| Git 'git clone' Lets Remote Users Execute Arbitrary Code When Cloning to a Target System - SecurityTracker | SECTRACK | www.security |
| UNCONFIRMED: Git Submodule Arbitrary Code Execution (PoC) - Linux local Exploit | EXPLOIT-DB | www.exploit-c |

| | | |
|--|---------|--|
| USN-3/91-1: Git vulnerability Ubuntu security notices | UBUNTU | usn.ubuntu.com |
| fsck: detect submodule urls starting with dash · git/git@a124133 · GitHub | MISC | github.com |
| Git CVE-2018-17456 Arbitrary Code Execution Vulnerability | BID | www.securityfocus.com |
| fsck: detect submodule paths starting with dash · git/git@1a7fd1f · GitHub | MISC | github.com |
| Red Hat Customer Portal | REDHAT | access.redhat.com |
| oss-security - CVE-2018-17456 Git RCE via .gitmodules | MISC | www.openwall.com |
| Bugtraq: March 2019 Sourcetree Advisory - Multiple Remote Code Execution Vulnerabilities | BUGTRAQ | seclists.org |
| CVE Program record | CVE.ORG | www.cve.org |
| NVD vulnerability detail | NVD | nvd.nist.gov |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[500218](#) Alpine Linux Security Update for git

[503962](#) Alpine Linux Security Update for git

© [CVE.report](https://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](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org/cve). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report