



CVE-2016-10129

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

Summary

CVE	CVE-2016-10129
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-24 15:59:00 UTC
Updated	2017-03-28 01:59:00 UTC
Description	The Git Smart Protocol support in libgit2 before 0.24.6 and 0.25.x before 0.25.1 allows remote attackers to cause a denial of service (CPU consumption) via crafted requests.

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Libgit2 Project	Libgit2	0.25.0	All	All	All
Application	Libgit2 Project	Libgit2	0.25.0	rc1	All	All
Application	Libgit2 Project	Libgit2	0.25.0	rc2	All	All
Application	Libgit2 Project	Libgit2	All	All	All	All
Application	Libgit2 Project	Libgit2	0.25.0	All	All	All
Application	Libgit2 Project	Libgit2	0.25.0	rc1	All	All
Application	Libgit2 Project	Libgit2	0.25.0	rc2	All	All

References

Reference	Source	Link	Tags
openSUSE-SU-2017:0484-1: moderate: Security update for libgit2	SUSE	lists.opensuse.org	Third Party Advisory
libgit2	CONFIRM	libgit2.github.com	Patch, Vendor Advisory
oss-security - CVE Request: two security fixes in libgit2 0.25.1, 0.24.6	MLIST	www.openwall.com	Mailing List, Patch, Vendor Advisory
openSUSE-SU-2017:0397-1: moderate: Security update for libgit2	SUSE	lists.opensuse.org	Third Party Advisory
smart_pkt: treat empty packet lines as error · libgit2/libgit2@84d30d5 · GitHub	CONFIRM	github.com	Issue Tracking, Patch, Vendor Advisory
oss-security - Re: CVE Request: two security fixes in libgit2 0.25.1, 0.24.6	MLIST	www.openwall.com	Mailing List, Patch, Vendor Advisory
libgit2 Multiple NULL Pointer Dereference Remote Code Execution Vulnerability	BID	www.securityfocus.com	

openSUSE-SU-2017:0405-1: moderate: Security update for libgit2	SUSE	lists.opensuse.org	Third Party Advisory
smart_pkt: treat empty packet lines as error · libgit2/libgit2@2fdef64 · GitHub	CONFIRM	github.com	Issue Tracking, Patch
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

- [501035](#) Alpine Linux Security Update for libgit2
- [501600](#) Alpine Linux Security Update for libgit2-1.0
- [502109](#) Alpine Linux Security Update for libgit2-1.1
- [504998](#) Alpine Linux Security Update for libgit2

© [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](#)