



CVE-2018-15501

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

Summary

CVE	CVE-2018-15501
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-08-18 02:29:00 UTC
Updated	2022-05-11 20:59:00 UTC
Description	In ng_pkt in transports/smart_pkt.c in libgit2 before 0.26.6 and 0.27.x before 0.27.4, a remote attacker can send a crafted s

Risk And Classification

Problem Types: CWE-125

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Libgit2	Libgit2	All	All	All	All
Application	Libgit2	Libgit2	All	All	All	All

References

Reference	Source	Link
Bug 1104641 – VUL-0: CVE-2018-15501: libgit2: out-of-bounds reads when processing smart-protocol "ng" packets	MISC	bugzilla.su
[SECURITY] [DLA 2936-1] libgit2 security update	MLIST	lists.debian
[SECURITY] [DLA 1477-1] libgit2 security update	MLIST	lists.debian
Sicherheit: Denial of Service in libgit2 - Pro-Linux	MISC	www.pro-l
9406 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	MISC	bugs.chro
Release libgit2 v0.27.4 · libgit2/libgit2 · GitHub	MISC	github.com
Release libgit2 v0.26.6 · libgit2/libgit2 · GitHub	MISC	github.com
smart_pkt: fix potential OOB-read when processing ng packet · libgit2/libgit2@1f9a851 · GitHub	MISC	github.com
CVE Program record	CVE.ORG	www.cve.c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[179136](#) Debian Security Update for libgit2 (DLA 2936-1)

[501037](#) Alpine Linux Security Update for libgit2

[501602](#) Alpine Linux Security Update for libgit2-1.0

[502111](#) Alpine Linux Security Update for libgit2-1.1

© [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](#)