



# CVE-2016-10128

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

## Summary

<b>CVE</b>	CVE-2016-10128
<b>State</b>	PUBLIC
<b>Assigner</b>	security@debian.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-03-24 15:59:00 UTC
<b>Updated</b>	2017-03-28 01:59:00 UTC
<b>Description</b>	Buffer overflow in the git_pkt_parse_line function in transports/smart_pkt.c in the Git Smart Protocol support in libgit2 before

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Libgit2 Project</a>	<a href="#">Libgit2</a>	0.25.0	All	All	All
Application	<a href="#">Libgit2 Project</a>	<a href="#">Libgit2</a>	0.25.0	rc1	All	All
Application	<a href="#">Libgit2 Project</a>	<a href="#">Libgit2</a>	0.25.0	rc2	All	All
Application	<a href="#">Libgit2 Project</a>	<a href="#">Libgit2</a>	All	All	All	All
Application	<a href="#">Libgit2 Project</a>	<a href="#">Libgit2</a>	0.25.0	All	All	All
Application	<a href="#">Libgit2 Project</a>	<a href="#">Libgit2</a>	0.25.0	rc1	All	All
Application	<a href="#">Libgit2 Project</a>	<a href="#">Libgit2</a>	0.25.0	rc2	All	All

## References

Reference	Source	Link	Tags
libgit2 'smart_pkt.c' Buffer Overflow Vulnerability	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>	
smart_pkt: verify packet length exceeds PKT_LEN_SIZE · libgit2/libgit2@4ac39c7 · GitHub	CONFIRM	<a href="https://github.com">github.com</a>	Issue Tr
openSUSE-SU-2017:0484-1: moderate: Security update for libgit2	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Third Pa
libgit2	CONFIRM	<a href="https://libgit2.github.com">libgit2.github.com</a>	Patch, V
oss-security - CVE Request: two security fixes in libgit2 0.25.1, 0.24.6	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing L
openSUSE-SU-2017:0397-1: moderate: Security update for libgit2	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Third Pa
oss-security - Re: CVE Request: two security fixes in libgit2 0.25.1, 0.24.6	MLIST	<a href="http://www.openwall.com">www.openwall.com</a>	Mailing L

smart_pkt: verify packet length exceeds PKT_LEN_SIZE · libgit2/libgit2@66e3774 · GitHub	CONFIRM	<a href="https://github.com">github.com</a>	Issue Tr
openSUSE-SU-2017:0405-1: moderate: Security update for libgit2	SUSE	<a href="https://lists.opensuse.org">lists.opensuse.org</a>	Third Pa
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonica
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonica

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](#)