



CVE-2016-7567

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

Summary

CVE	CVE-2016-7567
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-23 21:59:00 UTC
Updated	2020-04-29 13:26:00 UTC
Description	Buffer overflow in the SLPFoldWhiteSpace function in common/slp_compare.c in OpenSLP 2.0 allows remote attackers to f

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openslp	Openslp	2.0.0	-	All	All
Application	Openslp	Openslp	2.0.0	-	All	All

References

Reference	Source	Link	Tags
OpenSLP: Multiple vulnerabilities (GLSA 201707-05) — Gentoo Security	GENTOO	security.gentoo.org	Third Party Advisory
OpenSLP 2.0.0 - Multiple Vulnerabilities - Linux local Exploit	EXPLOIT-DB	www.exploit-db.com	Third Party Advisory, V
OpenSLP / Code / Commit [34fb3a]	CONFIRM	sourceforge.net	Third Party Advisory
oss-security - Re: CVE Request - OpenSLP 2.0 Memory Corruption	MLIST	www.openwall.com	Mailing List, Third Party
OpenSLP 'common/slp_compare.c' Remote Buffer Overflow Vulnerability	BID	www.securityfocus.com	Third Party Advisory, V
oss-security - CVE Request - OpenSLP 2.0 Memory Corruption	MLIST	www.openwall.com	Mailing List, Patch, Thir
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

[710514](#) Gentoo Linux OpenSLP Multiple Vulnerabilities (GLSA 201707-05)

[901181](#) Common Base Linux Mariner (CBL-Mariner) Security Update for openslp (7320)

[904649](#) Common Base Linux Mariner (CBL-Mariner) Security Update for openslp (7320-1)

© [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](#)