



# CVE-2015-3276

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2015-3276
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2015-12-07 20:59:00 UTC
<b>Updated</b>	2023-04-28 18:28:00 UTC
<b>Description</b>	The nss_parse_ciphers function in libraries/libldap/tls_m.c in OpenLDAP does not properly parse OpenSSL-style multi-keyw

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Openldap</a>	<a href="#">Openldap</a>	All	All	All	All
Application	<a href="#">Openldap</a>	<a href="#">Openldap</a>	All	All	All	All
Operating System	<a href="#">Oracle</a>	<a href="#">Linux</a>	7	-	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Desktop</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Eus</a>	7.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Hpc Node</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.6	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Aus</a>	7.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

Reference	Source	Link
<a href="#">access.redhat.com   CVE-2015-3276</a>	MISC	<a href="#">access.redhat.</a>
<a href="#">OpenLDAP Cipherstring Parsing Bug Lets Remote Users Downgrade the Encryption Cipher - SecurityTracker</a>	SECTRACK	<a href="#">www.securitytr</a>
<a href="#">Red Hat Customer Portal</a>	REDHAT	<a href="#">rhn.redhat.com</a>
<a href="#">Bug 1238322 – CVE-2015-3276 openldap: incorrect multi-keyword mode cipherstring parsing</a>	CONFIRM	<a href="#">bugzilla.redhat</a>
<a href="#">Oracle Linux Bulletin - October 2015</a>	CONFIRM	<a href="#">www.oracle.co</a>
<a href="#">Red Hat Customer Portal</a>	MISC	<a href="#">access.redhat.</a>
<a href="#">CVE Program record</a>	CVE.ORG	<a href="#">www.cve.org</a>
<a href="#">NVD vulnerability detail</a>	NVD	<a href="#">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- [900160](#) CBL-Mariner Linux Security Update for openldap 2.4.57
- [901187](#) Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (6770-1)
- [903586](#) Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (2546)

© [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](#)