



CVE-2013-4449

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

Summary

CVE	CVE-2013-4449
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-02-05 18:55:00 UTC
Updated	2016-12-08 03:03:00 UTC
Description	The rwm overlay in OpenLDAP 2.4.23, 2.4.36, and earlier does not properly count references, which allows remote attackers

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Openldap	Openldap	2.4.10	All	All	All
Application	Openldap	Openldap	2.4.11	All	All	All
Application	Openldap	Openldap	2.4.12	All	All	All
Application	Openldap	Openldap	2.4.13	All	All	All
Application	Openldap	Openldap	2.4.14	All	All	All
Application	Openldap	Openldap	2.4.15	All	All	All
Application	Openldap	Openldap	2.4.16	All	All	All
Application	Openldap	Openldap	2.4.17	All	All	All
Application	Openldap	Openldap	2.4.18	All	All	All
Application	Openldap	Openldap	2.4.19	All	All	All
Application	Openldap	Openldap	2.4.20	All	All	All
Application	Openldap	Openldap	2.4.21	All	All	All
Application	Openldap	Openldap	2.4.22	All	All	All

Application	Openldap	Openldap	2.4.23	All	All	All
Application	Openldap	Openldap	2.4.24	All	All	All
Application	Openldap	Openldap	2.4.25	All	All	All
Application	Openldap	Openldap	2.4.26	All	All	All
Application	Openldap	Openldap	2.4.27	All	All	All
Application	Openldap	Openldap	2.4.28	All	All	All
Application	Openldap	Openldap	2.4.29	All	All	All
Application	Openldap	Openldap	2.4.30	All	All	All
Application	Openldap	Openldap	2.4.31	All	All	All
Application	Openldap	Openldap	2.4.32	All	All	All
Application	Openldap	Openldap	2.4.33	All	All	All
Application	Openldap	Openldap	2.4.34	All	All	All
Application	Openldap	Openldap	2.4.35	All	All	All
Application	Openldap	Openldap	2.4.6	All	All	All
Application	Openldap	Openldap	2.4.7	All	All	All
Application	Openldap	Openldap	2.4.8	All	All	All
Application	Openldap	Openldap	2.4.9	All	All	All
Application	Openldap	Openldap	2.4.10	All	All	All
Application	Openldap	Openldap	2.4.11	All	All	All
Application	Openldap	Openldap	2.4.12	All	All	All
Application	Openldap	Openldap	2.4.13	All	All	All
Application	Openldap	Openldap	2.4.14	All	All	All
Application	Openldap	Openldap	2.4.15	All	All	All
Application	Openldap	Openldap	2.4.16	All	All	All
Application	Openldap	Openldap	2.4.17	All	All	All
Application	Openldap	Openldap	2.4.18	All	All	All
Application	Openldap	Openldap	2.4.19	All	All	All
Application	Openldap	Openldap	2.4.20	All	All	All
Application	Openldap	Openldap	2.4.21	All	All	All
Application	Openldap	Openldap	2.4.22	All	All	All
Application	Openldap	Openldap	2.4.23	All	All	All
Application	Openldap	Openldap	2.4.24	All	All	All
Application	Openldap	Openldap	2.4.25	All	All	All
Application	Openldap	Openldap	2.4.26	All	All	All
Application	Openldap	Openldap	2.4.27	All	All	All

Application	Openldap	Openldap	2.4.28	All	All	All
Application	Openldap	Openldap	2.4.29	All	All	All
Application	Openldap	Openldap	2.4.30	All	All	All
Application	Openldap	Openldap	2.4.31	All	All	All
Application	Openldap	Openldap	2.4.32	All	All	All
Application	Openldap	Openldap	2.4.33	All	All	All
Application	Openldap	Openldap	2.4.34	All	All	All
Application	Openldap	Openldap	2.4.35	All	All	All
Application	Openldap	Openldap	2.4.6	All	All	All
Application	Openldap	Openldap	2.4.7	All	All	All
Application	Openldap	Openldap	2.4.8	All	All	All
Application	Openldap	Openldap	2.4.9	All	All	All
Application	Openldap	Openldap	All	All	All	All

References

Reference

Red Hat Customer Portal

OpenLDAP 'rwm_conn_destroy' Denial of Service Vulnerability

2016-04 Security Bulletin: CTP Series: Multiple vulnerabilities in CTP Series - Juniper Networks

Full Disclosure: APPLE-SA-2019-12-10-3 macOS Catalina 10.15.2, Security Update 2019-002 Mojave, Security Update 2019-007 High Sierra

oss-security - Re: CVE request: slapd segfaults on certain queries with rwm overlay enabled

Support / Security / Advisories // MDVSA-2014:026 | Mandriva

OpenLDAP ITS - Incoming/7723

Cisco Unified Communications Manager Denial of Service Vulnerability

About the security content of macOS Catalina 10.15.2, Security Update 2019-002 Mojave, Security Update 2019-007 High Sierra - Apple Support

Debian -- Security Information -- DSA-3209-1 openldap

Oracle VM Server for x86 Bulletin - July 2016

Bug 1019490 – CVE-2013-4449 openldap: segfault on certain queries with rwm overlay

OpenLDAP RWM Overlay Reference Counting Flaw Lets Remote Users Deny Service - SecurityTracker

Red Hat Customer Portal

Juniper Networks - 2015-10 Security Bulletin: CTPView: Multiple Vulnerabilities in CTPView

Bugtraq: APPLE-SA-2019-12-10-3 macOS Catalina 10.15.2, Security Update 2019-002 Mojave, Security Update 2019-007 High Sierra

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)