



CVE-2021-27212

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

Summary

CVE	CVE-2021-27212
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-02-14 03:15:00 UTC
Updated	2023-11-07 03:31:00 UTC
Description	In OpenLDAP through 2.4.57 and 2.5.x through 2.5.1alpha, an assertion failure in slapd can occur in the issuerAndThisUpd

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Openldap	Openldap	2.5.0	alpha	All	All
Application	Openldap	Openldap	2.5.1	alpha	All	All
Application	Openldap	Openldap	2.5.0	alpha	All	All
Application	Openldap	Openldap	2.5.1	alpha	All	All
Application	Openldap	Openldap	All	All	All	All

References

Reference

- [bookkeeper-issues] 20210628 [GitHub] [bookkeeper] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade to 9.0
- Pony Mail!
- 9454 – A malicious packet can force OpenLDAP to fail an assertion and crash (schema_init.c:3808: checkTime)
- [SECURITY] [DLA 2574-1] openldap security update
- Debian -- Security Information -- DSA-4860-1 openldap

[ITS#9454 fix issuerAndThisUpdateCheck \(9badb734\)](#) · [Commits](#) · [openldap](#) / [OpenLDAP](#) · [GitLab](#)

[CVE-2021-27212 OpenLDAP Vulnerability in NetApp Products](#) | [NetApp Product Security](#)

Pony Mail!

[\[bookkeeper-issues\] 20210629 \[GitHub\] \[bookkeeper\] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade](#)

[ITS#9454 fix issuerAndThisUpdateCheck \(3539fc33\)](#) · [Commits](#) · [openldap](#) / [OpenLDAP](#) · [GitLab](#)

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[174780](#) SUSE Enterprise Linux Security update for openldap2 (SUSE-SU-2021:0692-1)

[174783](#) SUSE Enterprise Linux Security update for openldap2 (SUSE-SU-2021:0723-1)

[174918](#) SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2021:14700-1)

[180396](#) Debian Security Update for openldap (CVE-2021-27212)

[354907](#) Amazon Linux Security Advisory for openldap : ALAS2-2023-2033

[354925](#) Amazon Linux Security Advisory for openldap : ALAS-2023-1741

[355082](#) Amazon Linux Security Advisory for openldap : AL2012-2023-407

[355117](#) Amazon Linux Security Advisory for openldap : ALAS2023-2023-177

[500481](#) Alpine Linux Security Update for openldap

[501460](#) Alpine Linux Security Update for openldap

[504240](#) Alpine Linux Security Update for openldap

[591406](#) Siemens SIMATIC S7-1500 CPU GNU/Linux subsystem Multiple Vulnerabilities (SSB-439005, ICSA-22-104-13)

[670252](#) EulerOS Security Update for openldap (EulerOS-SA-2021-1824)

[670318](#) EulerOS Security Update for openldap (EulerOS-SA-2021-1906)

[670343](#) EulerOS Security Update for openldap (EulerOS-SA-2021-1881)

[670371](#) EulerOS Security Update for openldap (EulerOS-SA-2021-1954)

[670392](#) EulerOS Security Update for openldap (EulerOS-SA-2021-1933)

[670657](#) EulerOS Security Update for openldap (EulerOS-SA-2021-2415)

[670923](#) EulerOS Security Update for openldap (EulerOS-SA-2021-1933)

[750317](#) OpenSUSE Security Update for openldap2 (openSUSE-SU-2021:0408-1)

900160 CBL-Mariner Linux Security Update for openldap 2.4.57
901932 Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (6771-1)
902849 Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (3886)

© [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](#)