



CVE-2020-36223

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

Summary

CVE	CVE-2020-36223
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-26 18:15:00 UTC
Updated	2023-11-07 03:22:00 UTC
Description	A flaw was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Values Return Filter control handling, res

Risk And Classification

Problem Types: CWE-125 | CWE-415

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	All	All	All	All
Operating System	Apple	Mac Os X	All	All	All	All
Operating System	Apple	Mac Os X	10.14.6	-	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-004	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-005	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-006	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2019-007	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-001	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-002	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-003	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-004	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-005	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-006	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2020-007	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2021-001	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2021-002	All	All
Operating System	Apple	Mac Os X	10.14.6	security_update_2021-003	All	All

Operating System	Apple	Mac Os X	10.14.6	supplemental_update	All	All
Operating System	Apple	Mac Os X	10.14.6	supplemental_update_2	All	All
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	All	All	All	All
Application	Openldap	Openldap	All	All	All	All

References

Reference

[OPENLDAP_REL_ENG_2_4_57 · Tags · openldap / OpenLDAP · GitLab](#)

[\[bookkeeper-issues\] 20210628 \[GitHub\] \[bookkeeper\] padma81 opened a new issue #2746: Security Vulnerabilities in CentOS 7 image, Upgrade](#)

Pony Mail!

[About the security content of macOS Big Sur 11.4 - Apple Support](#)

[9408 -- Double free of vrFilter causes segfault due to out of bounds read](#)

[Debian -- Security Information -- DSA-4845-1 openldap](#)

[ITS#9408 fix vrfilter double-free \(21981053\) · Commits · openldap / OpenLDAP · GitLab](#)

[Full Disclosure: APPLE-SA-2021-05-25-3 Security Update 2021-004 Mojave](#)

[Full Disclosure: APPLE-SA-2021-05-25-4 Security Update 2021-003 Catalina](#)

[February 2021 OpenLDAP Vulnerabilities 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](#)

[About the security content of Security Update 2021-003 Catalina - Apple Support](#)

[Full Disclosure: APPLE-SA-2021-05-25-2 macOS Big Sur 11.4](#)

[\[SECURITY\] \[DLA 2544-1\] openldap security update](#)

[About the security content of Security Update 2021-004 Mojave - Apple Support](#)

[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)
296069 Oracle Solaris 11.4 Support Repository Update (SRU) 31.88.5 Missing (CPUJAN2021)
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
375585 Apple macOS Security Update 2021-004 Mojave (HT212531)
375586 Apple macOS Security Update 2021-003 Catalina (HT212530)
375588 Apple MacOS Big Sur 11.4 Not Installed (HT212529)
501459 Alpine Linux Security Update for openldap
504239 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)
670305 EulerOS Security Update for compat-openldap (EulerOS-SA-2021-1771)
670308 EulerOS Security Update for compat-openldap (EulerOS-SA-2021-1916)
670318 EulerOS Security Update for openldap (EulerOS-SA-2021-1906)
670343 EulerOS Security Update for openldap (EulerOS-SA-2021-1881)
670603 EulerOS Security Update for compat-openldap (EulerOS-SA-2021-2361)
670657 EulerOS Security Update for openldap (EulerOS-SA-2021-2415)
730121 McAfee Web Gateway Multiple Vulnerabilities (WP-3484,WP-3744,WP-3745,WP-3746,WP-3747,WP-3793,WP-3800)
750317 OpenSUSE Security Update for openldap2 (openSUSE-SU-2021:0408-1)
900145 CBL-Mariner Linux Security Update for openldap 2.4.50
903145 Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (3809)

© [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](#)