



CVE-2020-25692

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

Summary

CVE	CVE-2020-25692
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-08 01:15:00 UTC
Updated	2022-10-12 14:27:00 UTC
Description	A NULL pointer dereference was found in OpenLDAP server and was fixed in openldap 2.4.55, during a request for renami

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netapp	Cloud Backup	-	All	All	All
Hardware	Netapp	Solidfire Baseboard Management Controller	-	All	All	All
Operating System	Netapp	Solidfire Baseboard Management Controller Firmware	-	All	All	All
Application	Openldap	Openldap	All	All	All	All
Application	Openldap	Openldap	All	All	All	All
Operating System	Redhat	Enterprise Linux	5.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

References

Reference	Source	Link
1894567 – (CVE-2020-25692) CVE-2020-25692 openldap: NULL pointer dereference for unauthenticated packet in slapd	CONFIRM	bugz
CVE-2020-25692 OpenLDAP Vulnerability in NetApp Products NetApp Product Security	CONFIRM	secu
CVE Program record	CVE.ORG	www
NVD vulnerability detail	NVD	nvd.

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[159169](#) Oracle Enterprise Linux Security Update for openldap (ELSA-2021-1389)

[239251](#) Red Hat Update for openldap (RHSA-2021:1389)

[352373](#) Amazon Linux Security Advisory for openldap: ALAS2-2021-1638

[377233](#) Alibaba Cloud Linux Security Update for openldap (ALINUX2-SA-2021:0023)

[500480](#) Alpine Linux Security Update for openldap

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

[670194](#) EulerOS Security Update for openldap (EulerOS-SA-2021-1693)

[670856](#) EulerOS Security Update for openldap (EulerOS-SA-2021-1157)

[750600](#) OpenSUSE Security Update for openldap2 (openSUSE-SU-2020:1918-1)

[750602](#) OpenSUSE Security Update for openldap2 (openSUSE-SU-2020:1920-1)

[900109](#) CBL-Mariner Linux Security Update for openldap 2.4.50

[902896](#) Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (3653)

© [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](#)