CVE-2022-29155

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2022-29155
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-04 20:15:00 UTC
Updated	2022-10-06 15:56:00 UTC
Description	In OpenLDAP 2.x before 2.5.12 and 2.6.x before 2.6.2, a SQL injection vulnerability exists in the experimental back-sql bac

Risk And Classification

Problem Types: CWE-89

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	11.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Hardware	Netapp	H300s	-	All	All	All
Operating System	Netapp	H300s Firmware	-	All	All	All
Hardware	Netapp	H410c	-	All	All	All
Operating System	Netapp	H410c Firmware	-	All	All	All
Hardware	Netapp	H410s	-	All	All	All
Operating System	Netapp	H410s Firmware	-	All	All	All
Hardware	Netapp	H500s	-	All	All	All
Operating System	Netapp	H500s Firmware	-	All	All	All
Hardware	Netapp	H700e	-	All	All	All
Operating System	Netapp	H700e Firmware	-	All	All	All
Hardware	Netapp	H700s	-	All	All	All
Operating System	Netapp	H700s Firmware	-	All	All	All
Application	Openldap	Openldap	All	All	All	All

References

Reference	Source	Link	Tags
CVE-2022-29155 OpenLDAP Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	
[SECURITY] [DLA 3017-1] openldap security update	MLIST	lists.debian.org	
9815 – Serious SQL injection vulnerability in back-sql	MISC	bugs.openldap.org	
Debian -- Security Information -- DSA-5140-1 openldap	DEBIAN	www.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

179300 Debian Security Update for openldap (DSA 5140-1)

179312 Debian Security Update for openldap (DLA 3017-1)

182921 Debian Security Update for openldap (CVE-2022-29155)

198791 Ubuntu Security Notification for OpenLDAP Vulnerability (USN-5424-1)

353938 Amazon Linux Security Advisory for openldap : ALAS-2022-1586

353939 Amazon Linux Security Advisory for openldap : ALAS2-2022-1796

354630 Amazon Linux Security Advisory for openldap : AL2012-2022-362

501974 Alpine Linux Security Update for openldap

504241 Alpine Linux Security Update for openldap

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

671843 EulerOS Security Update for compat-openldap (EulerOS-SA-2022-1885)

671856 EulerOS Security Update for openldap (EulerOS-SA-2022-1908)

671897 EulerOS Security Update for openldap (EulerOS-SA-2022-1942)

671919 EulerOS Security Update for openldap (EulerOS-SA-2022-2005)

671953 EulerOS Security Update for openldap (EulerOS-SA-2022-1975)

671987 EulerOS Security Update for openldap (EulerOS-SA-2022-2141)

672006 EulerOS Security Update for openldap (EulerOS-SA-2022-2166)

672232 EulerOS Security Update for openldap (EulerOS-SA-2022-2628)

672233 EulerOS Security Update for compat-openldap (EulerOS-SA-2022-2604)

752127 SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2022:1685-1)

752131 SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2022:1671-1)

752134 SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2022:1670-1)

752160 SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2022:1771-1)

752171 SUSE Enterprise Linux Security Update for openldap2 (SUSE-SU-2022:1832-1)

901322 Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (9678)

901666 Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (9672)

902326 Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (9672-1)

904810 Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (9678-1)

905915 Common Base Linux Mariner (CBL-Mariner) Security Update for openldap (9678-2)