



CVE-2020-28935

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

Summary

CVE	CVE-2020-28935
State	PUBLIC
Assigner	sep@nlnetlabs.nl
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-07 22:15:00 UTC
Updated	2023-03-29 15:15:00 UTC
Description	NLnet Labs Unbound, up to and including version 1.12.0, and NLnet Labs NSD, up to and including version 4.3.3, contain a

Risk And Classification

Problem Types: CWE-59

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Nlnetlabs	Name Server Daemon	All	All	All	All
Application	Nlnetlabs	Name Server Daemon	All	All	All	All
Application	Nlnetlabs	Unbound	All	All	All	All
Application	Nlnetlabs	Unbound	All	All	All	All

References

Reference	Source	Link	Tags
www.nlnetlabs.nl/downloads/unbound/CVE-2020-28935.txt	CONFIRM	www.nlnetlabs.nl	Vendor Advisory
[SECURITY] [DLA 2556-1] unbound1.9 security update	MLIST	lists.debian.org	
NSD: Symbolic link traversal (GLSA 202101-38) — Gentoo security	GENTOO	security.gentoo.org	Third Party Advisory
[SECURITY] [DLA 3371-1] unbound security update	MLIST	lists.debian.org	
www.nlnetlabs.nl/downloads/nsd/CVE-2020-28935.txt	CONFIRM	www.nlnetlabs.nl	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

Vendor Comments And Credit

LEGACY: We would like to thank Mason Loring Bliss for bringing the issue to our attention.

Legacy QID Mappings

159223 Oracle Enterprise Linux Security Update for unbound (ELSA-2021-1853)
181641 Debian Security Update for unbound (DLA 3371-1)
198356 Ubuntu Security Notification for Unbound vulnerabilities (USN-4938-1)
239293 Red Hat Update for unbound (RHSA-2021:1853)
240098 Red Hat Update for unbound (RHSA-2022:0632)
352454 Amazon Linux Security Advisory for unbound: ALAS2-2021-1683
500452 Alpine Linux Security Update for nsd
504218 Alpine Linux Security Update for nsd
670210 EulerOS Security Update for unbound (EulerOS-SA-2021-1709)
670218 EulerOS Security Update for unbound (EulerOS-SA-2021-1857)
670678 EulerOS Security Update for unbound (EulerOS-SA-2021-2436)
690392 Free Berkeley Software Distribution (FreeBSD) Security Update for unbound/nsd (388ebb5b-3c95-11eb-929d-d4c9ef517024)
750496 OpenSUSE Security Update for nsd (openSUSE-SU-2020:2222-1)
750497 OpenSUSE Security Update for nsd (openSUSE-SU-2020:2222-1)
751647 SUSE Enterprise Linux Security Update for unbound (SUSE-SU-2022:0176-1)
751664 OpenSUSE Security Update for unbound (openSUSE-SU-2022:0176-1)
751682 SUSE Enterprise Linux Security Update for unbound (SUSE-SU-2022:0301-1)
900237 CBL-Mariner Linux Security Update for unbound 1.10.0
901823 Common Base Linux Mariner (CBL-Mariner) Security Update for unbound (6931-1)
903302 Common Base Linux Mariner (CBL-Mariner) Security Update for unbound (3654)
940041 AlmaLinux Security Update for unbound (ALSA-2021:1853)
960747 Rocky Linux Security Update for unbound (RLSA-2021:1853)

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](#)