



CVE-2020-8623

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

Summary

CVE	CVE-2020-8623
State	PUBLIC
Assigner	security-officer@isc.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-08-21 21:15:00 UTC
Updated	2023-11-07 03:26:00 UTC
Description	In BIND 9.10.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.10.5-S1 -> 9.11.21-S1 of the BIND 9 Supported

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Isc	Bind	9.10.5	s1	All	All
Application	Isc	Bind	9.11.21	s1	All	All
Application	Isc	Bind	9.10.5	s1	All	All
Application	Isc	Bind	9.11.21	s1	All	All
Application	Isc	Bind	All	All	All	All
Application	Isc	Bind	All	All	All	All
Application	Isc	Bind	All	All	All	All
Application	Netapp	Steelstore Cloud Integrated Storage	-	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All

Operating System	Opensuse	Leap	15.2	All	All	All
Application	Synology	Dns Server	All	All	All	All

References

Reference	Source
[security-announce] openSUSE-SU-2020:1699-1: moderate: Security update f	SUSE
USN-4468-1: Bind vulnerabilities Ubuntu security notices Ubuntu	UBUNTU
BIND: Multiple vulnerabilities (GLSA 202008-19) — Gentoo security	GENTOO
[SECURITY] [DLA 2355-1] bind9 security update	MLIST
[SECURITY] Fedora 31 Update: bind-dyndb-ldap-11.2-4.fc31 - package-announce - Fedora Mailing-Lists	FEDORA
Debian -- Security Information -- DSA-4752-1 bind9	DEBIAN
[security-announce] openSUSE-SU-2020:1701-1: moderate: Security update f	SUSE
[SECURITY] Fedora 32 Update: bind-9.11.22-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA
August 2020 ISC BIND Vulnerabilities in NetApp Products NetApp Product Security	CONFIR
[SECURITY] Fedora 32 Update: bind-9.11.22-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA
Synology Inc.	CONFIR
CVE-2020-8623: A flaw in native PKCS#11 code can lead to a remotely triggerable assertion failure in pk11.c - Security Advisories	CONFIR
[SECURITY] Fedora 31 Update: bind-dyndb-ldap-11.2-4.fc31 - package-announce - Fedora Mailing-Lists	FEDORA
CVE Program record	CVE.OP
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: ISC would like to thank Lyu Chiy for bringing this vulnerability to our attention.

Legacy QID Mappings

377151 Alibaba Cloud Linux Security Update for bind (ALINUX3-SA-2021:0025)
377309 Alibaba Cloud Linux Security Update for bind (ALINUX2-SA-2020:0181)
378294 Virtuozzo Linux Security Update for bind-pkcs11-libs (VZLSA-2020:5011)
500064 Alpine Linux Security Update for bind
503743 Alpine Linux Security Update for bind
900157 CBL-Mariner Linux Security Update for bind 9.16.3
903040 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (1990)

© [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](#)