



CVE-2021-25219

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

Summary

CVE	CVE-2021-25219
State	PUBLIC
Assigner	security-officer@isc.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-10-27 21:15:00 UTC
Updated	2023-11-07 03:31:00 UTC
Description	In BIND 9.3.0 -> 9.11.35, 9.12.0 -> 9.16.21, and versions 9.9.3-S1 -> 9.11.35-S1 and 9.16.8-S1 -> 9.16.21-S1 of BIND Sup

Risk And Classification

Problem Types: NVD-CWE-noinfo

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
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	34	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Application	Isc	Bind	All	All	All	All
Application	Isc	Bind	9.10.5	s1	All	All
Application	Isc	Bind	9.10.7	s1	All	All
Application	Isc	Bind	9.11.12	s1	All	All
Application	Isc	Bind	9.11.21	s1	All	All
Application	Isc	Bind	9.11.27	s1	All	All
Application	Isc	Bind	9.11.29	s1	All	All
Application	Isc	Bind	9.11.3	s1	All	All
Application	Isc	Bind	9.11.35	s1	All	All
Application	Isc	Bind	9.11.5	s3	All	All
Application	Isc	Bind	9.11.5	s5	All	All

[SECURITY] Fedora 34 Update: bind-9.16.22-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
CVE-2021-25219 ISC BIND Vulnerability in NetApp Products NetApp Product Security	CONFIRM	security.netapp.com
[SECURITY] Fedora 33 Update: bind-9.11.36-1.fc33 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Oracle Critical Patch Update Advisory - April 2022	MISC	www.oracle.com
[SECURITY] Fedora 35 Update: bind-9.16.22-1.fc35 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
ISC BIND: Multiple Vulnerabilities (GLSA 202210-25) — Gentoo security	GENTOO	security.gentoo.org
[SECURITY] Fedora 34 Update: bind-9.16.22-1.fc34 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 35 Update: bind-9.16.22-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 33 Update: bind-9.11.36-1.fc33 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf	CONFIRM	cert-portal.siemens.com
[SECURITY] [DLA 2807-1] bind9 security update	MLIST	lists.debian.org
CVE-2021-25219: Lame cache can be abused to severely degrade resolver performance - Security Advisories	CONFIRM	kb.isc.org
Debian -- Security Information -- DSA-4994-1 bind9	DEBIAN	www.debian.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: ISC would like to thank Kishore Kumar Kothapalli of Infoblox for bringing this vulnerability to our attention.

Legacy QID Mappings

- [15128](#) ISC BIND Lame cache Vulnerability
- [159815](#) Oracle Enterprise Linux Security Update for bind (ELSA-2022-2092)
- [178855](#) Debian Security Update for bind9 (DSA 4994-1)
- [178863](#) Debian Security Update for bind9 (DLA 2807-1)
- [183695](#) Debian Security Update for bind9 (CVE-2021-25219)
- [198558](#) Ubuntu Security Notification for Bind Vulnerability (USN-5126-1)
- [240291](#) Red Hat Update for bind security (RHSA-2022:2092)
- [282051](#) Fedora Security Update for bind (FEDORA-2021-eb8dab50ba)
- [282052](#) Fedora Security Update for bind (FEDORA-2021-39b33260b8)
- [296066](#) Oracle Solaris 11.4 Support Repository Update (SRU) 40.107.3 Missing (CPUOCT2021)
- [330098](#) IBM AIX BIND Denial of Service (DoS) Vulnerability (bind_advisory20)

376031 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) BIND Vulnerability (K77326807)
376049 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) BIND Vulnerability (K77326807)
500062 Alpine Linux Security Update for bind
501382 Alpine Linux Security Update for bind
501948 Alpine Linux Security Update for bind
503871 Alpine Linux Security Update for bind
671192 EulerOS Security Update for bind (EulerOS-SA-2022-1001)
671208 EulerOS Security Update for bind (EulerOS-SA-2022-1021)
671307 EulerOS Security Update for bind (EulerOS-SA-2022-1237)
671324 EulerOS Security Update for bind (EulerOS-SA-2022-1249)
671356 EulerOS Security Update for bind (EulerOS-SA-2022-1261)
671663 EulerOS Security Update for bind (EulerOS-SA-2022-1705)
672329 EulerOS Security Update for dhcp (EulerOS-SA-2022-2759)
672358 EulerOS Security Update for dhcp (EulerOS-SA-2022-2724)
672424 EulerOS Security Update for dhcp (EulerOS-SA-2022-2842)
672461 EulerOS Security Update for dhcp (EulerOS-SA-2022-2817)
672477 EulerOS Security Update for dhcp (EulerOS-SA-2023-1032)
672510 EulerOS Security Update for dhcp (EulerOS-SA-2023-1007)
710661 Gentoo Linux ISC BIND Multiple Vulnerabilities (GLSA 202210-25)
751363 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:3657-1)
751396 OpenSUSE Security Update for bind (openSUSE-SU-2021:3773-1)
751400 OpenSUSE Security Update for bind (openSUSE-SU-2021:1502-1)
751635 OpenSUSE Security Update for bind (openSUSE-SU-2022:0151-1)
751980 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2022:0151-1)
752457 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2022:2713-1)
901647 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (6327)
902239 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (6327-1)
940543 AlmaLinux Security Update for bind (ALSA-2022-2092)

960283 Rocky Linux Security Update for bind (RLSA-2022:2092)

© [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](#)