# CVE-2021-25215

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2021-25215 |
| **State** | PUBLIC |
| **Assigner** | security-officer@isc.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2021-04-29 01:15:00 UTC |
| **Updated** | 2023-11-07 03:31:00 UTC |
| **Description** | In BIND 9.0.0 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIN |

## Risk And Classification

**Problem Types:** CWE-617

## 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 | 9.0 | All | All | All |
| Operating System | Fedoraproject | Fedora | 33 | All | All | All |
| Operating System | Fedoraproject | Fedora | 34 | 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 | 9.11.5 | s3 | All | All |
| Application | Isc | Bind | 9.11.5 | s5 | All | All |
| Application | Isc | Bind | 9.11.5 | s6 | All | All |
| Application | Isc | Bind | 9.11.6 | s1 | All | All |
| Application | Isc | Bind | 9.11.7 | s1 | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Isc | Bind | 9.11.8 | s1 | All | All |
| Application | Isc | Bind | 9.16.11 | s1 | All | All |
| Application | Isc | Bind | 9.16.13 | s1 | All | All |
| Application | Isc | Bind | 9.16.8 | s1 | All | All |
| Application | Isc | Bind | 9.9.12 | s1 | All | All |
| Application | Isc | Bind | 9.9.13 | s1 | All | All |
| Application | Isc | Bind | 9.9.3 | s1 | All | All |
| Hardware | Netapp | 500f | - | All | All | All |
| Operating System | Netapp | 500f Firmware | - | All | All | All |
| Hardware | Netapp | A250 | - | All | All | All |
| Operating System | Netapp | A250 Firmware | - | All | All | All |
| Application | Netapp | Active Iq Unified Manager | - | All | All | All |
| Application | Netapp | Cloud Backup | - | All | All | All |
| Hardware | Netapp | H300e | - | All | All | All |
| Operating System | Netapp | H300e Firmware | - | All | All | All |
| Hardware | Netapp | H300s | - | All | All | All |
| Operating System | Netapp | H300s Firmware | - | All | All | All |
| Hardware | Netapp | H410s | - | All | All | All |
| Operating System | Netapp | H410s Firmware | - | All | All | All |
| Hardware | Netapp | H500e | - | All | All | All |
| Operating System | Netapp | H500e 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 | Oracle | Tekelec Platform Distribution | All | All | All | All |
| Application | Siemens | Sinec Infrastructure Network Services | All | All | All | All |

## References

| Reference |
|---|
| April 2021 ISC BIND Vulnerabilities in NetApp Products \| NetApp Product Security |
| oss-security - Re: ISC discloses three BIND vulnerabilities (CVE-2021-25214, CVE-2021-25215, and CVE-2021-25216) |
| [SECURITY] Fedora 34 Update: bind-dyndb-ldap-11.7-3.fc34 - package-announce - Fedora Mailing-Lists |

| |
|---|
| [SECURITY] Fedora 33 Update: bind-9.11.31-1.fc33 - package-announce - Fedora Mailing-Lists |
| Oracle Critical Patch Update Advisory - October 2021 |
| [SECURITY] Fedora 34 Update: bind-dyndb-ldap-11.7-3.fc34 - package-announce - Fedora Mailing-Lists |
| cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf |
| Debian -- Security Information -- DSA-4909-1 bind9 |
| oss-security - ISC discloses three BIND vulnerabilities (CVE-2021-25214, CVE-2021-25215, and CVE-2021-25216) |
| [SECURITY] [DLA 2647-1] bind9 security update |
| [SECURITY] Fedora 33 Update: bind-9.11.31-1.fc33 - package-announce - Fedora Mailing-Lists |
| CVE-2021-25215: An assertion check can fail while answering queries for DNAME records that require the DNAME to be processed to resolve |
| oss-security - Re: ISC discloses three BIND vulnerabilities (CVE-2021-25214, CVE-2021-25215, and CVE-2021-25216) |
| oss-security - Re: ISC discloses three BIND vulnerabilities (CVE-2021-25214, CVE-2021-25215, and CVE-2021-25216) |
| CVE Program record |
| NVD vulnerability detail |

## Vendor Comments And Credit

Discovery Credit

**LEGACY:** ISC would like to thank Siva Kakarla for bringing this vulnerability to our attention.

## Legacy QID Mappings

- 15126 ISC BIND Assertion Failure Vulnerability
- 159171 Oracle Enterprise Linux Security Update for bind (ELSA-2021-1469)
- 159174 Oracle Enterprise Linux Security Update for bind (ELSA-2021-9213)
- 159232 Oracle Enterprise Linux Security Update for bind (ELSA-2021-1989)
- 174977 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:1469-1)
- 174978 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:1471-1)
- 174979 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:1468-1)
- 178573 Debian Security Update for bind9 (DSA 4909-1)
- 178593 Debian Security Update for bind9 (DSA 4909-1)
- 178594 Debian Security Update for bind9 (DLA 2647-1)
- 180392 Debian Security Update for bind9 (CVE-2021-25215)
- 198348 Ubuntu Security Notification for Bind vulnerabilities (USN-4929-1)
- 239267 Red Hat Update for bind (RHSA-2021:1478)

239268 Red Hat Update for bind (RHSA-2021:1477)

239269 Red Hat Update for bind (RHSA-2021:1469)

239279 Red Hat Update for bind (RHSA-2021:2028)

239283 Red Hat Update for bind (RHSA-2021:2024)

239284 Red Hat Update for bind (RHSA-2021:1989)

257082 CentOS Security Update for bind (CESA-2021:1469)

281228 Fedora Security Update for bind (FEDORA-2021-47f23870ec)

281229 Fedora Security Update for bind (FEDORA-2021-ace61cbee1)

296068 Oracle Solaris 11.4 Support Repository Update (SRU) 34.94.4 Missing (CPUAPR2021)

330085 IBM AIX BIND Denial of Service Vulnerability (bind_advisory19)

352376 Amazon Linux Security Advisory for bind: ALAS2-2021-1635

352483 Amazon Linux Security Advisory for bind: ALAS-2021-1508

375664 F5 BIG-IP ASM,LTM,APM BIG-IP BIND Vulnerability (K96223611)

377078 Alibaba Cloud Linux Security Update for bind (ALINUX2-SA-2021:0026)

500060 Alpine Linux Security Update for bind

503740 Alpine Linux Security Update for bind

670424 EulerOS Security Update for bind (EulerOS-SA-2021-1975)

670478 EulerOS Security Update for bind (EulerOS-SA-2021-2236)

670504 EulerOS Security Update for bind (EulerOS-SA-2021-2262)

670562 EulerOS Security Update for bind (EulerOS-SA-2021-2320)

670596 EulerOS Security Update for bind (EulerOS-SA-2021-2354)

671133 EulerOS Security Update for bind (EulerOS-SA-2021-2572)

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)

730121 McAfee Web Gateway Multiple Vulnerabilities (WP-3484,WP-3744,WP-3745,WP-3746,WP-3747,WP-3793,WP-3800)

750091 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:1826-1)

750231 OpenSUSE Security Update for bind (openSUSE-SU-2021:0668-1)

750804 OpenSUSE Security Update for bind (openSUSE-SU-2021:1826-1)

900029 CBL-Mariner Linux Security Update for bind 9.16.3

902997 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (4170)

940043 AlmaLinux Security Update for bind (ALSA-2021:1989)

960049 Rocky Linux Security Update for bind (RLSA-2021:1989)

© 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 registred 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**