



CVE-2023-3341

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

Summary

CVE	CVE-2023-3341
State	PUBLIC
Assigner	security-officer@isc.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-09-20 13:15:00 UTC
Updated	2024-01-31 00:15:00 UTC
Description	The code that processes control channel messages sent to `named` calls certain functions recursively during packet parsing

Risk And Classification

Problem Types: CWE-787

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	9.11.3	s4	All	All
Application	isc	Bind	9.11.35	s1	All	All
Application	isc	Bind	9.11.37	s1	All	All
Application	isc	Bind	9.11.4	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	9.16.12	s1	All	All
Application	Isc	Bind	9.16.13	s1	All	All
Application	Isc	Bind	9.16.14	s1	All	All
Application	Isc	Bind	9.16.21	s1	All	All
Application	Isc	Bind	9.16.32	s1	All	All
Application	Isc	Bind	9.16.36	s1	All	All
Application	Isc	Bind	9.16.43	s1	All	All
Application	Isc	Bind	9.16.8	s1	All	All
Application	Isc	Bind	9.18.0	s1	All	All
Application	Isc	Bind	9.18.18	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

References

Reference	Source	Link
oss-security - ISC has disclosed two vulnerabilities in BIND 9 (CVE-2023-3341, CVE-2023-4236)	MISC	www.openwall.com
[SECURITY] [DLA 3726-1] bind9 security update		lists.debian.org
Debian -- Security Information -- DSA-5504-1 bind9	MISC	www.debian.org
[SECURITY] Fedora 38 Update: bind-dyndb-ldap-11.10-21.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
CVE-2023-3341 ISC BIND Vulnerability in NetApp Products NetApp Product Security	MISC	security.netapp.com
CVE-2023-3341	MISC	kb.isc.org
[SECURITY] Fedora 39 Update: bind-9.18.19-1.fc39 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
[SECURITY] Fedora 37 Update: bind-dyndb-ldap-11.10-17.fc37 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[160955](#) Oracle Enterprise Linux Security Update for bind (ELSA-2023-5474)

[160956](#) Oracle Enterprise Linux Security Update for bind9.16 (ELSA-2023-5460)

[160975](#) Oracle Enterprise Linux Security Update for bind (ELSA-2023-5691)

160983 Oracle Enterprise Linux Security Update for bind (ELSA-2023-5689)
199772 Ubuntu Security Notification for Bind Vulnerabilities (USN-6390-1)
199818 Ubuntu Security Notification for Bind Vulnerability (USN-6421-1)
242103 Red Hat Update for bind9.16 (RHSA-2023:5460)
242104 Red Hat Update for bind (RHSA-2023:5474)
242117 Red Hat Update for bind (RHSA-2023:5473)
242127 Red Hat Update for bind (RHSA-2023:5526)
242131 Red Hat Update for bind (RHSA-2023:5529)
242134 Red Hat Update for bind (RHSA-2023:5527)
242161 Red Hat Update for bind (RHSA-2023:5691)
242163 Red Hat Update for bind (RHSA-2023:5689)
242164 Red Hat Update for bind (RHSA-2023:5690)
242180 Red Hat Update for bind9.16 (RHSA-2023:5771)
257260 CentOS Security Update for bind
257280 CentOS Security Update for bind (CESA-2023:5691)
284550 Fedora Security Update for bind (FEDORA-2023-a2621f58a9)
284608 Fedora Security Update for bind (FEDORA-2023-87502c4a93)
285243 Fedora Security Update for bind (FEDORA-2023-b4acb0f7c6)
296105 Oracle Solaris 11.4 Support Repository Update (SRU) 63.157.1 Missing (CPUOCT2023)
330156 IBM AIX Denial of Service (DoS) ISC BIND Vulnerability (bind_advisory25)
356359 Amazon Linux Security Advisory for bind : ALAS-2023-1845
356380 Amazon Linux Security Advisory for bind : ALAS2023-2023-372
356401 Amazon Linux Security Advisory for bind : ALAS2-2023-2273
356992 Amazon Linux Security Advisory for bind : AL2012-2023-476
378960 Alibaba Cloud Linux Security Update for bind (ALINUX3-SA-2023:0126)
379090 IBM QRadar SIEM Multiple Security Vulnerabilities (7070736)
503353 Alpine Linux Security Update for bind
503354 Alpine Linux Security Update for bind

505853 Alpine Linux Security Update for bind
6000219 Debian Security Update for bind9 (DSA 5504-1)
6000457 Debian Security Update for bind9 (DLA 3726-1)
673441 EulerOS Security Update for bind (EulerOS-SA-2023-3199)
673554 EulerOS Security Update for bind (EulerOS-SA-2023-3164)
673627 EulerOS Security Update for bind (EulerOS-SA-2024-1256)
673770 EulerOS Security Update for bind (EulerOS-SA-2023-3235)
673793 EulerOS Security Update for bind (EulerOS-SA-2023-3263)
673806 EulerOS Security Update for bind (EulerOS-SA-2024-1132)
673910 EulerOS Security Update for bind (EulerOS-SA-2023-3291)
674056 EulerOS Security Update for bind (EulerOS-SA-2023-3323)
754912 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2023:3737-1)
754930 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2023:3796-1)
754944 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2023:3805-1)
754969 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2023:3821-1)
755008 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2023:3934-1)
907369 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (29943-1)
941277 AlmaLinux Security Update for bind9.16 (ALSA-2023:5460)
941281 AlmaLinux Security Update for bind (ALSA-2023:5474)
941293 AlmaLinux Security Update for bind (ALSA-2023:5689)
961047 Rocky Linux Security Update for bind (RLSA-2023:5689)

© [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](#)