



CVE-2022-3080

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

Summary

CVE	CVE-2022-3080
State	PUBLIC
Assigner	security-officer@isc.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-09-21 11:15:00 UTC
Updated	2023-11-07 03:50:00 UTC
Description	By sending specific queries to the resolver, an attacker can cause named to crash.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	isc	Bind	All	All	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

References

Reference
FEDORA-2022-8268735e06
oss-security - ISC has disclosed six vulnerabilities in BIND (CVE-2022-2795, CVE-2022-2881, CVE-2022-2906, CVE-2022-3080, CVE-2022-3081)
Debian -- Security Information -- DSA-5235-1 bind9
[SECURITY] Fedora 36 Update: bind-9.16.33-1.fc36 - package-announce - Fedora Mailing-Lists
ISC BIND: Multiple Vulnerabilities (GLSA 202210-25) — Gentoo security
CVE-2022-3080: BIND 9 resolvers configured to answer from stale cache
[SECURITY] Fedora 35 Update: bind-dyndb-ldap-11.9-16.fc35 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 37 Update: bind-9.18.7-1.fc37 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 37 Update: bind-9.18.7-1.fc37 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 37 Update: bind-9.18.7-1.fc37 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 35 Update: bind-dyndb-ldap-11.9-16.fc35 - package-announce - Fedora Mailing-Lists

CVE Program record

NVD vulnerability detail



Vendor Comments And Credit

Discovery Credit

LEGACY: ISC would like to thank Maksym Odintsev for bringing this vulnerability to our attention.

Legacy QID Mappings

15138 ISC BIND Assertion Failure Vulnerability
160119 Oracle Enterprise Linux Security Update for bind (ELSA-2022-6763)
160126 Oracle Enterprise Linux Security Update for bind9.16 (ELSA-2022-6781)
181072 Debian Security Update for bind9 (DSA 5235-1)
183301 Debian Security Update for bind9 (CVE-2022-3080)
198945 Ubuntu Security Notification for Bind Vulnerabilities (USN-5626-1)
240702 Red Hat Update for bind (RHSA-2022:6763)
240703 Red Hat Update for bind9.16 (RHSA-2022:6781)
283150 Fedora Security Update for bind (FEDORA-2022-8268735e06)
283158 Fedora Security Update for bind (FEDORA-2022-b197d64471)
296084 Oracle Solaris 11.4 Support Repository Update (SRU) 50.126.3 Missing (CPUOCT2022)
330122 IBM AIX Denial of Service (DoS) ISC BIND Vulnerability (bind_advisory22)
355145 Amazon Linux Security Advisory for bind : ALAS2023-2023-161
502507 Alpine Linux Security Update for bind
502711 Alpine Linux Security Update for bind
672503 EulerOS Security Update for bind (EulerOS-SA-2023-1002)
672524 EulerOS Security Update for bind (EulerOS-SA-2023-1027)
710661 Gentoo Linux ISC BIND Multiple Vulnerabilities (GLSA 202210-25)
752737 SUSE Enterprise Linux Recommended update for bind (SUSE-SU-2022:3767-1)

904037 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (11009)
904040 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (11000)
904547 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (11009-1)
904633 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (11000-1)
940673 AlmaLinux Security Update for bind9.16 (ALSA-2022:6781)
940679 AlmaLinux Security Update for bind (ALSA-2022:6763)
960351 Rocky Linux Security Update for bind9.16 (RLSA-2022:6781)
960475 Rocky Linux Security Update for bind (RLSA-2022:6763)

© [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](#)