



CVE-2022-38177

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

Summary

CVE	CVE-2022-38177
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 spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small me

Risk And Classification

Problem Types: CWE-401

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	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	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	9.11.14-s1	All	All	All
Application	isc	Bind	9.11.19-s1	All	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	9.11.37	s1	All	All
Application	isc	Bind	9.11.5	s3	All	All

Application	lsc	Bind	9.11.5	s3	All	All
Application	lsc	Bind	9.11.5	s5	All	All
Application	lsc	Bind	9.11.5	s6	All	All
Application	lsc	Bind	9.11.6	s1	All	All
Application	lsc	Bind	9.11.7	s1	All	All
Application	lsc	Bind	9.11.8	s1	All	All
Application	lsc	Bind	9.16.11	s1	All	All
Application	lsc	Bind	9.16.13	s1	All	All
Application	lsc	Bind	9.16.21	s1	All	All
Application	lsc	Bind	9.16.32	s1	All	All
Application	lsc	Bind	9.16.8	s1	All	All
Application	lsc	Bind	9.9.12	s1	All	All
Application	lsc	Bind	9.9.13	s1	All	All
Application	lsc	Bind	9.9.3	s1	All	All
Application	lsc	Bind	9.9.3	s1	All	All
Application	lsc	Bind	All	All	All	All
Application	Netapp	Active Iq Unified Manager	-	All	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-2022-3

Debian -- Security Information -- DSA-5235-1 bind9

[SECURITY] Fedora 36 Update: bind-9.16.33-1.fc36 - package-announce - Fedora Mailing-Lists

[SECURITY] [DLA 3138-1] bind9 security update

ISC BIND: Multiple Vulnerabilities (GLSA 202210-25) — Gentoo security

CVE-2022-38177 ISC BIND Vulnerability in NetApp Products | NetApp Product Security

[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

CVE-2022-38177: Memory leak in ECDSA DNSSEC verification code

[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

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

15137 ISC BIND Memory Leak Vulnerability (CVE-2022-38177)
160119 Oracle Enterprise Linux Security Update for bind (ELSA-2022-6763)
160122 Oracle Enterprise Linux Security Update for bind (ELSA-2022-6765)
160125 Oracle Enterprise Linux Security Update for bind (ELSA-2022-6778)
160126 Oracle Enterprise Linux Security Update for bind9.16 (ELSA-2022-6781)
181072 Debian Security Update for bind9 (DSA 5235-1)
181112 Debian Security Update for bind9 (DLA 3138-1)
184369 Debian Security Update for bind9 (CVE-2022-38177)
198945 Ubuntu Security Notification for Bind Vulnerabilities (USN-5626-1)
240701 Red Hat Update for bind (RHSA-2022:6765)
240702 Red Hat Update for bind (RHSA-2022:6763)
240703 Red Hat Update for bind9.16 (RHSA-2022:6781)
240706 Red Hat Update for bind (RHSA-2022:6778)
240707 Red Hat Update for bind (RHSA-2022:6780)
240708 Red Hat Update for bind (RHSA-2022:6779)
257195 CentOS Security Update for bind (CESA-2022:6765)
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)
354835 Amazon Linux Security Advisory for bind : ALAS2-2023-2001
355145 Amazon Linux Security Advisory for bind : ALAS2023-2023-161
377619 Alibaba Cloud Linux Security Update for bind (ALINUX2-SA-2022:0043)
377669 F5 BIG-IP Bind vulnerability cve-2022-38177 (K27155546)
502507 Alpine Linux Security Update for bind
502711 Alpine Linux Security Update for bind

672407 EulerOS Security Update for bind (EulerOS-SA-2022-2788)
672439 EulerOS Security Update for bind (EulerOS-SA-2022-2838)
672456 EulerOS Security Update for bind (EulerOS-SA-2022-2813)
672477 EulerOS Security Update for dhcp (EulerOS-SA-2023-1032)
672503 EulerOS Security Update for bind (EulerOS-SA-2023-1002)
672510 EulerOS Security Update for dhcp (EulerOS-SA-2023-1007)
672524 EulerOS Security Update for bind (EulerOS-SA-2023-1027)
672534 EulerOS Security Update for bind (EulerOS-SA-2023-1117)
672543 EulerOS Security Update for bind (EulerOS-SA-2023-1093)
672629 EulerOS Security Update for dhcp (EulerOS-SA-2023-1353)
672652 EulerOS Security Update for dhcp (EulerOS-SA-2023-1381)
672781 EulerOS Security Update for bind (EulerOS-SA-2023-1489)
673277 EulerOS Security Update for dhcp (EulerOS-SA-2023-2580)
673317 EulerOS Security Update for dhcp (EulerOS-SA-2023-2610)
710661 Gentoo Linux ISC BIND Multiple Vulnerabilities (GLSA 202210-25)
752651 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2022:3499-1)
752699 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2022:3682-1)
752717 SUSE Enterprise Linux Security Update for bind (SUSE-SU-2022:3729-1)
752737 SUSE Enterprise Linux Recommended update for bind (SUSE-SU-2022:3767-1)
904039 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (11010)
904041 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (11001)
904540 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (11010-1)
904645 Common Base Linux Mariner (CBL-Mariner) Security Update for bind (11001-1)
940670 AlmaLinux Security Update for bind (ALSA-2022:6778)
940673 AlmaLinux Security Update for bind9.16 (ALSA-2022:6781)
940679 AlmaLinux Security Update for bind (ALSA-2022:6763)
960290 Rocky Linux Security Update for bind (RLSA-2022:6778)
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](#)