



# CVE-2023-2911

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-2911
<b>State</b>	PUBLIC
<b>Assigner</b>	security-officer@isc.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-06-21 17:15:00 UTC
<b>Updated</b>	2023-07-03 19:09:00 UTC
<b>Description</b>	If the `recursive-clients` quota is reached on a BIND 9 resolver configured with both `stale-answer-enable yes;` and `stale-a

## Risk And Classification

**Problem Types:** CWE-787

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	11.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	12.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	37	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	38	All	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	All	All	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	All	All	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	All	All	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	All	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H300s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410c</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410c Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H410s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H410s Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H500s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500s Firmware</a>	-	All	All	All

Hardware	<a href="#">Netapp</a>	H700s	-	All	All	All
Operating System	<a href="#">Netapp</a>	H700s Firmware	-	All	All	All

## References

Reference	Source	Link
[SECURITY] Fedora 37 Update: bind-dyndb-ldap-11.10-15.fc37 - package-announce - Fedora Mailing-Lists	MISC	<a href="https://lists.fedoraproject.org/">lists.fedoraproject.</a>
CVE-2023-2911	MISC	<a href="https://kb.isc.org">kb.isc.org</a>
Debian -- Security Information -- DSA-5439-1 bind9	MISC	<a href="https://www.debian.org">www.debian.org</a>
oss-security - ISC has disclosed two vulnerabilities in BIND 9 (CVE-2023-2828, CVE-2023-2911)	MISC	<a href="https://www.openwall.com">www.openwall.com</a>
403 Forbidden	MISC	<a href="https://security.netapp.co">security.netapp.co</a>
[SECURITY] Fedora 38 Update: bind-dyndb-ldap-11.10-17.fc38 - package-announce - Fedora Mailing-Lists	MISC	<a href="https://lists.fedoraproject.org/">lists.fedoraproject.</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

<a href="#">15142</a> ISC BIND Denial of Service (DoS) Vulnerability (CVE-2023-2911)
<a href="#">199435</a> Ubuntu Security Notification for Bind Vulnerabilities (USN-6183-1)
<a href="#">284044</a> Fedora Security Update for bind (FEDORA-2023-8e1ddb1fa2)
<a href="#">284045</a> Fedora Security Update for bind (FEDORA-2023-c0ff5a2f68)
<a href="#">284113</a> Fedora Security Update for bind (FEDORA-2023-1d526d551c)
<a href="#">355628</a> Amazon Linux Security Advisory for bind : ALAS2023-2023-240
<a href="#">6000172</a> Debian Security Update for bind9 (DSA 5439-1)
<a href="#">673912</a> EulerOS Security Update for bind (EulerOS-SA-2023-2837)
<a href="#">673993</a> EulerOS Security Update for bind (EulerOS-SA-2023-2854)
<a href="#">907393</a> Common Base Linux Mariner (CBL-Mariner) Security Update for bind (27237-1)

© [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](#).

Free CVE JSON API [cve.report/api](https://cve.report/api)

CVE.report and Source URL Uptime Status [status.cve.report](https://status.cve.report)