



CVE-2022-3488

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

Summary

CVE	CVE-2022-3488
State	PUBLIC
Assigner	security-officer@isc.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-26 21:15:00 UTC
Updated	2023-11-07 03:51:00 UTC
Description	Processing of repeated responses to the same query, where both responses contain ECS pseudo-options, but where the fi

Risk And Classification

Problem Types: CWE-617

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	isc	Bind	9.11.37	s1	All	All
Application	isc	Bind	9.11.4	s1	All	All
Application	isc	Bind	9.16.36	s1	All	All
Application	isc	Bind	9.16.8	s1	All	All

References

Reference	Source	Link	Tags
CVE-2022-3488: BIND Supported Preview Edition named may terminate unex	MISC	kb.isc.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[15135](#) ISC BIND Assertion Failure Vulnerability

[355145](#) Amazon Linux Security Advisory for bind : ALAS2023-2023-161

© [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](#)