



# CVE-2022-0635

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

## Summary

<b>CVE</b>	CVE-2022-0635
<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>	2022-03-23 12:15:00 UTC
<b>Updated</b>	2023-11-09 14:44:00 UTC
<b>Description</b>	Versions affected: BIND 9.18.0 When a vulnerable version of named receives a series of specific queries, the named process

## Risk And Classification

**Problem Types:** CWE-617

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	isc	Bind	9.18.0	All	All	All
Hardware	Netapp	Baseboard Management Controller H300e	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H300e Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H300s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H300s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H410c	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H410c Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H410s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H410s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H500e	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H500e Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H500s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H500s Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H700e	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H700e Firmware	-	All	All	All
Hardware	Netapp	Baseboard Management Controller H700s	-	All	All	All
Operating System	Netapp	Baseboard Management Controller H700s Firmware	-	All	All	All

Hardware	<a href="#">Netapp</a>	<a href="#">H300e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H300e Firmware</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="#">H500e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H500e 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>	<a href="#">H700e</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700e Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">H700s</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">H700s Firmware</a>	-	All	All	All

## References

Reference	Source	Link	Tags
CVE-2022-0635: DNAME insist with synth-from-dnssec enabled - Security Advisories	CONFIRM	<a href="https://kb.isc.org">kb.isc.org</a>	
March 2022 ISC BIND Vulnerabilities in NetApp Products   NetApp Product Security	CONFIRM	<a href="https://security.netapp.com">security.netapp.com</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

## Vendor Comments And Credit

### Discovery Credit

**LEGACY:** ISC would like to thank Vincent Levigneron of AFNIC for reporting this issue to us and for verifying the fix and workaround.

## Legacy QID Mappings

[15131](#) ISC BIND Multiple Vulnerabilities

[183944](#) Debian Security Update for bind9 (CVE-2022-0635)

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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)