



# CVE-2021-25216

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2021-25216
<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>	2021-04-29 01:15:00 UTC
<b>Updated</b>	2022-05-03 16:04:00 UTC
<b>Description</b>	In BIND 9.5.0 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.11.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND

## Risk And Classification

**Problem Types:** CWE-125

## 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	9.0	All	All	All
Application	Isc	Bind	All	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	9.11.21	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	9.11.5	s3	All	All
Application	Isc	Bind	9.11.5	s5	All	All
Application	Isc	Bind	9.11.5	s6	All	All
Application	Isc	Bind	9.11.6	s1	All	All
Application	Isc	Bind	9.11.7	s1	All	All
Application	Isc	Bind	9.11.8	s1	All	All
Application	Isc	Bind	9.16.11	s1	All	All

Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.16.13	s1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.16.8	s1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.9.12	s1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.9.13	s1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.9.3	s1	All	All
Application	<a href="#">Netapp</a>	<a href="#">Active Iq Unified Manager</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Aff 500f</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Aff 500f Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">Aff A250</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">Aff A250 Firmware</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	-	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="#">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
Application	<a href="#">Siemens</a>	<a href="#">Sinec Infrastructure Network Services</a>	All	All	All	All

## References

### Reference

ZDI-21-657 | Zero Day Initiative

April 2021 ISC BIND Vulnerabilities in NetApp Products | NetApp Product Security

oss-security - Re: ISC discloses three BIND vulnerabilities (CVE-2021-25214, CVE-2021-25215, and CVE-2021-25216)

cert-portal.siemens.com/productcert/pdf/ssa-389290.pdf

Debian -- Security Information -- DSA-4909-1 bind9

oss-security - ISC discloses three BIND vulnerabilities (CVE-2021-25214, CVE-2021-25215, and CVE-2021-25216)

SECURITY: BIND 9.16.13 - CVE-2021-25214, CVE-2021-25215, and CVE-2021-25216

CVE-2021-25215: An assertion check can fail while answering queries for DNAME records that require the DNAME to be processed to resolve

oss-security - Re: ISC discloses three BIND vulnerabilities (CVE-2021-25214, CVE-2021-25215, and CVE-2021-25216)

oss-security - Re: ISC discloses three BIND vulnerabilities (CVE-2021-25214, CVE-2021-25215, and CVE-2021-25216)

CVE Program record

NVD vulnerability detail

### Vendor Comments And Credit

#### Discovery Credit

**LEGACY:** ISC would like to thank an anonymous party, working in conjunction with Trend Micro Zero Day Initiative, for reporting this issue to us.

### Legacy QID Mappings

[15124](#) ISC BIND Buffer Overflow Vulnerability

[174977](#) SUSE Enterprise Linux Security Update for bind (SUSE-SU-2021:1469-1)

[178573](#) Debian Security Update for bind9 (DSA 4909-1)

[178593](#) Debian Security Update for bind9 (DSA 4909-1)

[178594](#) Debian Security Update for bind9 (DLA 2647-1)

[179764](#) Debian Security Update for bind9 (CVE-2021-25216)

[198348](#) Ubuntu Security Notification for Bind vulnerabilities (USN-4929-1)

[296068](#) Oracle Solaris 11.4 Support Repository Update (SRU) 34.94.4 Missing (CPUAPR2021)

[500060](#) Alpine Linux Security Update for bind

[503740](#) Alpine Linux Security Update for bind

[730121](#) McAfee Web Gateway Multiple Vulnerabilities (WP-3484,WP-3744,WP-3745,WP-3746,WP-3747,WP-3793,WP-3800)

[900029](#) CBL-Mariner Linux Security Update for bind 9.16.3

[902859](#) Common Base Linux Mariner (CBL-Mariner) Security Update for bind (4177)

[904823](#) Common Base Linux Mariner (CBL-Mariner) Security Update for dhcp (12321)

[904991](#) Common Base Linux Mariner (CBL-Mariner) Security Update for dhcp (12482)

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](#)**