



# CVE-2020-8625

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

## Summary

<b>CVE</b>	CVE-2020-8625
<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>	2021-02-17 23:15:00 UTC
<b>Updated</b>	2023-11-07 03:26:00 UTC
<b>Description</b>	BIND servers are vulnerable if they are running an affected version and are configured to use GSS-TSIG features. In a con

## Risk And Classification

### Problem Types: CWE-120

## 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>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	10.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	9.0	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	34	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	33	All	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.21	s1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.27	s1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.3	s1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.5	s3	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.5	s5	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.6	s1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.7	s1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.8	s1	All	All

Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.16.11	s1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.16.8	s1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.17.0	All	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.17.1	All	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.11.21	s1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.11.27	s1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.11.3	s1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.11.5	s3	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.11.5	s5	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.11.6	s1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.11.7	s1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.11.8	s1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.16.11	s1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.16.8	s1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.17.0	All	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.17.1	All	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	All	All	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	All	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">500f</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">500f Firmware</a>	-	All	All	All
Hardware	<a href="#">Netapp</a>	<a href="#">A250</a>	-	All	All	All
Operating System	<a href="#">Netapp</a>	<a href="#">A250 Firmware</a>	-	All	All	All
Application	<a href="#">Netapp</a>	<a href="#">Cloud Backup</a>	-	All	All	All
Application	<a href="#">Siemens</a>	<a href="#">Sinec Infrastructure Network Services</a>	All	All	All	All

## References

### Reference

[SECURITY] Fedora 32 Update: bind-9.11.28-1.fc32 - package-announce - Fedora Mailing-Lists

CVE-2020-8625: A vulnerability in BIND's GSSAPI security policy negotiation can be targeted by a buffer overflow attack - Security Advisories  
 oss-security - BIND Operational Notification: Enabling the new BIND option "stale-answer-client-timeout" can result in unexpected server termi

[SECURITY] Fedora 33 Update: bind-9.11.28-1.fc33 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 32 Update: bind-9.11.28-1.fc32 - package-announce - Fedora Mailing-Lists

ZDI-21-195 | Zero Day Initiative

[SECURITY] [DLA 2568-1] bind9 security update

[SECURITY] Fedora 34 Update: bind-9.16.11-5.fc34 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 33 Update: bind-9.11.28-1.fc33 - package-announce - Fedora Mailing-Lists

oss-security - BIND Operational Notification: Zone journal (.jnl) file incompatibility,after upgrading to BIND 9.16.12 and 9.17

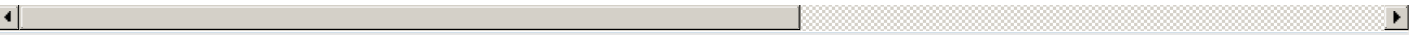
CVE-2020-8625 ISC BIND Vulnerability in NetApp Products | NetApp Product Security

[SECURITY] Fedora 34 Update: bind-9.16.11-5.fc34 - package-announce - Fedora Mailing-Lists

Debian -- Security Information -- DSA-4857-1 bind9

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

<a href="#">281600</a> Fedora Security Update for bind (FEDORA-2021-8b4744f152)
<a href="#">281607</a> Fedora Security Update for bind (FEDORA-2021-0595625865)
<a href="#">281608</a> Fedora Security Update for bind (FEDORA-2021-28f97e232d)
<a href="#">296069</a> Oracle Solaris 11.4 Support Repository Update (SRU) 31.88.5 Missing (CPUJAN2021)
<a href="#">352243</a> Amazon Linux Security Advisory for bind: ALAS-2021-1485
<a href="#">352252</a> Amazon Linux Security Advisory for bind: ALAS2-2021-1614
<a href="#">376869</a> Alibaba Cloud Linux Security Update for bind (ALINUX2-SA-2021:0011)
<a href="#">377151</a> Alibaba Cloud Linux Security Update for bind (ALINUX3-SA-2021:0025)
<a href="#">500059</a> Alpine Linux Security Update for bind
<a href="#">503739</a> Alpine Linux Security Update for bind
<a href="#">670330</a> EulerOS Security Update for bind (EulerOS-SA-2021-1894)
<a href="#">670359</a> EulerOS Security Update for bind (EulerOS-SA-2021-1865)
<a href="#">670364</a> EulerOS Security Update for bind (EulerOS-SA-2021-1766)
<a href="#">670386</a> EulerOS Security Update for bind (EulerOS-SA-2021-1939)
<a href="#">670431</a> EulerOS Security Update for bind (EulerOS-SA-2021-1918)
<a href="#">670596</a> EulerOS Security Update for bind (EulerOS-SA-2021-2354)
<a href="#">730228</a> McAfee Web Gateway Multiple Vulnerabilities (WP-3445, WP-3483, WP-3527, WP-3528, WP-3547, WP-3584,WP-3589,WP-

3611)

[750333](#) OpenSUSE Security Update for bind (openSUSE-SU-2021:0375-1)

[900065](#) CBL-Mariner Linux Security Update for bind 9.16.3

[903172](#) Common Base Linux Mariner (CBL-Mariner) Security Update for bind (3907)

[940192](#) AlmaLinux Security Update for bind (ALSA-2021:0670)

© [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](#)**