



# CVE-2020-8617

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

## Summary

<b>CVE</b>	CVE-2020-8617
<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>	2020-05-19 14:15:00 UTC
<b>Updated</b>	2023-11-07 03:26:00 UTC
<b>Description</b>	Using a specially-crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state if the att

## Risk And Classification

**Problem Types:** CWE-617

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	12.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	14.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	16.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	18.04	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	19.10	All	All	All
Operating System	<a href="#">Canonical</a>	<a href="#">Ubuntu Linux</a>	20.04	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>	8.0	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>	31	All	All	All
Operating System	<a href="#">Fedoraproject</a>	<a href="#">Fedora</a>	32	All	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.10.5	s1	All	All
Application	<a href="#">isc</a>	<a href="#">Bind</a>	9.10.7	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="#">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>	9.12.4	p1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.12.4	p2	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.3	s1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.10.5	s1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.10.7	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>	9.12.4	p1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.12.4	p2	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.3	s1	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
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
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
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
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.1	All	All	All
Operating System	<a href="#">Opensuse</a>	<a href="#">Leap</a>	15.2	All	All	All

## References

Reference	S
[security-announce] openSUSE-SU-2020:1699-1: moderate: Security update f	S
[SECURITY] Fedora 31 Update: bind-9.11.19-1.fc31 - package-announce - Fedora Mailing-Lists	F
CVE-2020-8617: A logic error in code which checks TSIG validity can be used to trigger an assertion failure in tsig.c - Security Advisories	C
BIND TSIG Denial Of Service ≈ Packet Storm	M
[SECURITY] [DLA 2227-1] bind9 security update	M
[SECURITY] [DLA 2227-1] bind9 security update	F

[SECURITY] Fedora 32 Update: bind-9.11.19-1.fc32 - package-announce - Fedora Mailing-Lists	F
[SECURITY] Fedora 31 Update: bind-9.11.19-1.fc31 - package-announce - Fedora Mailing-Lists	
oss-security - Two vulnerabilities disclosed in BIND (CVE-2020-8616 and CVE-2020-8617)	M
[security-announce] openSUSE-SU-2020:1701-1: moderate: Security update f	S
[SECURITY] Fedora 32 Update: bind-9.11.19-1.fc32 - package-announce - Fedora Mailing-Lists	
May 2020 ISC BIND Vulnerabilities in NetApp Products   NetApp Product Security	C
USN-4365-1: Bind vulnerabilities   Ubuntu security notices	L
USN-4365-2: Bind vulnerabilities   Ubuntu security notices	L
Debian -- Security Information -- DSA-4689-1 bind9	D
CVE Program record	C
NVD vulnerability detail	N

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

- [296074](#) Oracle Solaris 11.4 Support Repository Update (SRU) 22.69.4 Missing (CPUAPR2020)
- [377062](#) Alibaba Cloud Linux Security Update for bind (ALINUX2-SA-2020:0095)
- [377151](#) Alibaba Cloud Linux Security Update for bind (ALINUX3-SA-2021:0025)
- [390244](#) Oracle Managed Virtualization (VM) Server for x86 Security Update for bind (OVMSA-2020-0021)
- [500054](#) Alpine Linux Security Update for bind
- [503735](#) Alpine Linux Security Update for bind

© [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](#)