



# CVE-2017-3137

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

## Summary

<b>CVE</b>	CVE-2017-3137
<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>	2019-01-16 20:29:00 UTC
<b>Updated</b>	2019-10-09 23:27:00 UTC
<b>Description</b>	Mistaken assumptions about the ordering of records in the answer section of a response containing CNAME or DNAME res

## 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="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Operating System	<a href="#">Debian</a>	<a href="#">Debian Linux</a>	8.0	All	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.10.4	p6	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.10.5	b1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.10.5	rc1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.0	p3	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.1	b1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.1	rc1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.9.10	beta1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.9.10	rc1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.9.9	p6	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.9.9	s8	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.10.4	p6	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.10.5	b1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.10.5	rc1	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.0	p3	All	All
Application	<a href="#">Isc</a>	<a href="#">Bind</a>	9.11.1	b1	All	All

Application	Isc	Bind	9.11.1	rc1	All	All
Application	Isc	Bind	9.9.10	beta1	All	All
Application	Isc	Bind	9.9.10	rc1	All	All
Application	Isc	Bind	9.9.9	p6	All	All
Application	Isc	Bind	9.9.9	s8	All	All
Application	Netapp	Data Ontap Edge	-	All	All	All
Application	Netapp	Data Ontap Edge	-	All	All	All
Application	Netapp	Element Software	-	All	All	All
Application	Netapp	Element Software	-	All	All	All
Application	Netapp	Oncommand Balance	-	All	All	All
Application	Netapp	Oncommand Balance	-	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.5	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All

Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	6.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	6.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.4	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Eus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	6.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	6.5	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	6.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.2	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.3	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Server Tus</a>	7.6	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	6.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Enterprise Linux Workstation</a>	7.0	All	All	All

## References

### Reference

[CVE-2017-3137: A response packet can cause a resolver to terminate when processing an answer containing a CNAME or DNAME - Security](#)

[Debian -- Security Information -- DSA-3854-1 bind9](#)

[BIND CNAME/DNAME Record Processing Bug Lets Remote Users Cause the Target Service to Crash - SecurityTracker](#)

[Red Hat Customer Portal](#)

[April 2017 ISC BIND Vulnerabilities in NetApp Products | NetApp Product Security](#)

[BIND Recursion Processing Error in 'netaddr.c' Lets Remote Users Cause the Target 'named' Service to Crash - SecurityTracker](#)

[Red Hat Customer Portal](#)

Red Hat Customer Portal

ISC BIND CVE-2017-3137 Remote Denial of Service Vulnerability

BIND: Multiple vulnerabilities (GLSA 201708-01) — Gentoo Security

Red Hat Customer Portal

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

### Legacy QID Mappings

[378290](#) Virtuozzo Linux Security Update for bind-pkcs11-libs (VZLSA-2017:1095)

[378311](#) Virtuozzo Linux Security Update for bind-chroot (VZLSA-2017:1105)

[500048](#) Alpine Linux Security Update for bind

[503729](#) Alpine Linux Security Update for bind

[710473](#) Gentoo Linux BIND Multiple Vulnerabilities (GLSA 201708-01)

© [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](#)