# CVE-2017-3137

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2017-3137 |
| **State** | PUBLIC |
| **Assigner** | security-officer@isc.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2019-01-16 20:29:00 UTC |
| **Updated** | 2019-10-09 23:27:00 UTC |
| **Description** | 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 | Debian | Debian Linux | 8.0 | All | All | All |
| Operating System | Debian | Debian Linux | 8.0 | All | All | All |
| Application | Isc | Bind | 9.10.4 | p6 | All | All |
| Application | Isc | Bind | 9.10.5 | b1 | All | All |
| Application | Isc | Bind | 9.10.5 | rc1 | All | All |
| Application | Isc | Bind | 9.11.0 | p3 | All | All |
| Application | Isc | Bind | 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 | Isc | Bind | 9.10.4 | p6 | All | All |
| Application | Isc | Bind | 9.10.5 | b1 | All | All |
| Application | Isc | Bind | 9.10.5 | rc1 | All | All |
| Application | Isc | Bind | 9.11.0 | p3 | All | All |
| Application | Isc | Bind | 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 | Redhat | Enterprise Linux Server Eus | 6.7 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 6.7 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Eus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 6.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 6.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 6.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 6.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Tus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 6.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Workstation | 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) |