# CVE-2016-9131

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2016-9131 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2017-01-12 06:59:00 UTC |
| **Updated** | 2020-08-19 19:17:00 UTC |
| **Description** | named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to ca |

## Risk And Classification

**Problem Types:** CWE-20

## 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 | b2 | All | All |
| Application | Isc | Bind | 9.10.4 | b3 | All | All |
| Application | Isc | Bind | 9.10.4 | p2 | All | All |
| Application | Isc | Bind | 9.10.4 | p3 | All | All |
| Application | Isc | Bind | 9.10.4 | p4 | All | All |
| Application | Isc | Bind | 9.10.4 | rc1 | All | All |
| Application | Isc | Bind | 9.11.0 | a1 | All | All |
| Application | Isc | Bind | 9.11.0 | a2 | All | All |
| Application | Isc | Bind | 9.11.0 | a3 | All | All |
| Application | Isc | Bind | 9.11.0 | b1 | All | All |
| Application | Isc | Bind | 9.11.0 | b2 | All | All |
| Application | Isc | Bind | 9.11.0 | b3 | All | All |
| Application | Isc | Bind | 9.11.0 | p1 | All | All |
| Application | Isc | Bind | 9.11.0 | rc1 | All | All |
| Application | Isc | Bind | 9.9.9 | - | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Isc | Bind | 9.9.9 | b1 | All | All |
| Application | Isc | Bind | 9.9.9 | b2 | All | All |
| Application | Isc | Bind | 9.9.9 | p1 | All | All |
| Application | Isc | Bind | 9.9.9 | p3 | All | All |
| Application | Isc | Bind | 9.9.9 | p4 | All | All |
| Application | Isc | Bind | 9.10.4 | b2 | All | All |
| Application | Isc | Bind | 9.10.4 | b3 | All | All |
| Application | Isc | Bind | 9.10.4 | p2 | All | All |
| Application | Isc | Bind | 9.10.4 | p3 | All | All |
| Application | Isc | Bind | 9.10.4 | p4 | All | All |
| Application | Isc | Bind | 9.10.4 | rc1 | All | All |
| Application | Isc | Bind | 9.11.0 | a1 | All | All |
| Application | Isc | Bind | 9.11.0 | a2 | All | All |
| Application | Isc | Bind | 9.11.0 | a3 | All | All |
| Application | Isc | Bind | 9.11.0 | b1 | All | All |
| Application | Isc | Bind | 9.11.0 | b2 | All | All |
| Application | Isc | Bind | 9.11.0 | b3 | All | All |
| Application | Isc | Bind | 9.11.0 | p1 | All | All |
| Application | Isc | Bind | 9.11.0 | rc1 | All | All |
| Application | Isc | Bind | 9.9.9 | - | All | All |
| Application | Isc | Bind | 9.9.9 | b1 | All | All |
| Application | Isc | Bind | 9.9.9 | b2 | All | All |
| Application | Isc | Bind | 9.9.9 | p1 | All | All |
| Application | Isc | Bind | 9.9.9 | p3 | All | All |
| Application | Isc | Bind | 9.9.9 | p4 | All | All |
| Application | Isc | Bind | All | All | All | All |
| Application | Isc | Bind | All | All | All | All |
| Application | Netapp | Data Ontap Edge | - | All | All | All |
| Application | Netapp | Data Ontap Edge | - | All | All | All |
| Application | Netapp | Hci Management Node | - | All | All | All |
| Application | Netapp | Hci Management Node | - | All | All | All |
| Application | Netapp | Solidfire | - | All | All | All |
| Application | Netapp | Solidfire | - | All | All | All |
| Application | Netapp | Steelstore Cloud Integrated Storage | - | All | All | All |
| Application | Netapp | Steelstore Cloud Integrated Storage | - | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Desktop | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 7.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 7.7 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 7.2 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 7.3 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 7.4 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 7.5 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 7.6 | All | All | All |
| Operating System | Redhat | Enterprise Linux Eus | 7.7 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server | 7.0 | 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 | 7.7 | 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 | 7.7 | 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 | 7.7 | 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 | 7.7 | All | All | All |
| Operating System | Redhat | Enterprise Linux Server Workstation | 7.0 | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Operating System | Redhat | Enterprise Linux Server Workstation | 7.0 | All | All | All |

## References

| Reference |
|---|
| BIND Multiple Flaws Let Remote Users Cause the Target named Service to Stop Processing - SecurityTracker |
| ISC BIND CVE-2016-9131 Remote Denial of Service Vulnerability |
| Red Hat Customer Portal |
| February 2018 ISC BIND Vulnerabilities in NetApp Products \| NetApp Product Security |
| HPE Support document - HPE Support Center |
| Debian -- Security Information -- DSA-3758-1 bind9 |
| BIND: Multiple vulnerabilities (GLSA 201708-01) — Gentoo Security |
| CVE-2016-9131: A malformed response to an ANY query can cause an assertion failure during recursion \| Internet Systems Consortium Know |
| Red Hat Customer Portal |
| CVE Program record |
| NVD vulnerability detail |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

- 378219 Virtuozzo Linux Security Update for bind-pkcs11-devel (VZLSA-2017:0062)
- 500047 Alpine Linux Security Update for bind
- 503676 Alpine Linux Security Update for bind
- 505852 Alpine Linux Security Update for bind
- 710473 Gentoo Linux BIND Multiple Vulnerabilities (GLSA 201708-01)