



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 c

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

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)

© [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](#)