CVE-2014-0591

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2014-0591
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-01-14 04:29:56 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The query_findclosestnsec3 function in query.c in named in ISC BIND 9.6, 9.7, and 9.8 before 9.8.6-P2 and 9.9 before 9.9.

Risk And Classification

Primary CVSS: v2.0 2.6 from nvd@nist.gov

AV:N/AC:H/Au:N/C:N/I:N/A:P

EPSS: 0.515420000 probability, percentile 0.979050000 (date 2026-05-01)

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

High

Authentication

None

Confidentiality

None

Integrity

None

Availability

Partial

AV:N/AC:H/Au:N/C:N/I:N/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language

Application	Isc	Bind	9.6	All	All	All
Application	Isc	Bind	9.6	r5_p1	All	All
Application	Isc	Bind	9.6	r6_b1	All	All
Application	Isc	Bind	9.6	r6_rc1	All	All
Application	Isc	Bind	9.6	r6_rc2	All	All
Application	Isc	Bind	9.6	r7_p1	All	All
Application	Isc	Bind	9.6	r7_p2	All	All
Application	Isc	Bind	9.6	r9_p1	All	All
Application	Isc	Bind	9.6.0	All	All	All
Application	Isc	Bind	9.6.0	p1	All	All
Application	Isc	Bind	9.6.0	rc1	All	All
Application	Isc	Bind	9.6.0	rc2	All	All
Application	Isc	Bind	9.6.1	All	All	All
Application	Isc	Bind	9.6.1	p1	All	All
Application	Isc	Bind	9.6.1	p2	All	All
Application	Isc	Bind	9.6.1	p3	All	All
Application	Isc	Bind	9.6.1	rc1	All	All
Application	Isc	Bind	9.6.2	All	All	All
Application	Isc	Bind	9.6.2	rc1	All	All
Application	Isc	Bind	9.6.3	All	All	All
Application	Isc	Bind	9.6.3	rc1	All	All
Application	Isc	Bind	9.7.0	All	All	All
Application	Isc	Bind	9.7.0	b1	All	All
Application	Isc	Bind	9.7.0	p1	All	All
Application	Isc	Bind	9.7.0	p2	All	All
Application	Isc	Bind	9.7.0	rc1	All	All
Application	Isc	Bind	9.7.0	rc2	All	All
Application	Isc	Bind	9.7.1	All	All	All
Application	Isc	Bind	9.7.1	p1	All	All
Application	Isc	Bind	9.7.1	p2	All	All
Application	Isc	Bind	9.7.1	rc1	All	All
Application	Isc	Bind	9.7.2	All	All	All
Application	Isc	Bind	9.7.2	p1	All	All
Application	Isc	Bind	9.7.2	p2	All	All
Application	Isc	Bind	9.7.2	p3	All	All
Application	Isc	Bind	9.7.2	rc1	All	All

Application	Isc	Bind	9.7.2	rc1	All	All
Application	Isc	Bind	9.7.3	All	All	All
Application	Isc	Bind	9.7.3	b1	All	All
Application	Isc	Bind	9.7.3	p1	All	All
Application	Isc	Bind	9.7.3	rc1	All	All
Application	Isc	Bind	9.7.4	All	All	All
Application	Isc	Bind	9.7.4	b1	All	All
Application	Isc	Bind	9.7.4	p1	All	All
Application	Isc	Bind	9.7.4	rc1	All	All
Application	Isc	Bind	9.7.5	All	All	All
Application	Isc	Bind	9.7.5	b1	All	All
Application	Isc	Bind	9.7.5	rc1	All	All
Application	Isc	Bind	9.7.5	rc2	All	All
Application	Isc	Bind	9.7.6	All	All	All
Application	Isc	Bind	9.7.6	p1	All	All
Application	Isc	Bind	9.7.6	p2	All	All
Application	Isc	Bind	9.7.7	All	All	All
Application	Isc	Bind	9.8.0	All	All	All
Application	Isc	Bind	9.8.0	a1	All	All
Application	Isc	Bind	9.8.0	b1	All	All
Application	Isc	Bind	9.8.0	p1	All	All
Application	Isc	Bind	9.8.0	p2	All	All
Application	Isc	Bind	9.8.0	p4	All	All
Application	Isc	Bind	9.8.0	rc1	All	All
Application	Isc	Bind	9.8.1	All	All	All
Application	Isc	Bind	9.8.1	b1	All	All
Application	Isc	Bind	9.8.1	b2	All	All
Application	Isc	Bind	9.8.1	b3	All	All
Application	Isc	Bind	9.8.1	p1	All	All
Application	Isc	Bind	9.8.1	rc1	All	All
Application	Isc	Bind	9.8.2	b1	All	All
Application	Isc	Bind	9.8.2	rc1	All	All
Application	Isc	Bind	9.8.2	rc2	All	All
Application	Isc	Bind	9.8.3	All	All	All
Application	Isc	Bind	9.8.3	p1	All	All
Application	Isc	Bind	9.8.3	p2	All	All

Application	Isc	Bind	9.8.4	All	All	All
Application	Isc	Bind	9.8.5	All	All	All
Application	Isc	Bind	9.8.5	b1	All	All
Application	Isc	Bind	9.8.5	b2	All	All
Application	Isc	Bind	9.8.5	p1	All	All
Application	Isc	Bind	9.8.5	p2	All	All
Application	Isc	Bind	9.8.5	rc1	All	All
Application	Isc	Bind	9.8.5	rc2	All	All
Application	Isc	Bind	9.8.6	All	All	All
Application	Isc	Bind	9.8.6	b1	All	All
Application	Isc	Bind	9.8.6	p1	All	All
Application	Isc	Bind	9.8.6	rc1	All	All
Application	Isc	Bind	9.8.6	rc2	All	All
Application	Isc	Bind	9.9.4	All	All	All
Application	Isc	Bind	9.9.4	p1	All	All
Application	Isc	Bind	9.9.4	rc1	All	All
Application	Isc	Bind	9.9.4	rc2	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Sourc
Security Advisory SA56871 - SUSE update for bind - Secunia	af854a
Debian -- Security Information -- DSA-3023-1 bind9	af854a
Red Hat Customer Portal	af854a
[security-announce] SUSE-SU-2015:0480-1: important: Security update for	af854a
Security Advisory SA56425 - Ubuntu update for bind9 - Secunia	af854a
Security Advisory SA61199 - Red Hat update for bind97 - Secunia	af854a
404 Not Found	af854a
osvdb.org/101973	af854a
ISC BIND NSEC3-signed Zone Query Processing Flaw Lets Remote Users Deny Service - SecurityTracker	af854a
USN-2081-1: Bind vulnerability | Ubuntu	af854a
1051717 – (CVE-2014-0591) CVE-2014-0591 bind: named crash when handling malformed NSEC3-signed zones	af854a
'[security bulletin] HPSBUX02961 SSRT101420 rev.1 - HP-UX Running BIND, Remote Denial of Service (DoS' - MARC	af854a

About the security content of OS X Server v4.0 - Apple Support	af854a
The Slackware Linux Project: Slackware Security Advisories	af854a
ISC BIND NSEC3 Signed Zones Queries Handling Remote Denial of Service Vulnerability	af854a
Security Advisory SA56442 - ISC BIND NSEC3-Signed Zones Queries Handling Denial of Service Vulnerability - Secunia	af854a
Security Advisory SA56493 - FreeBSD update for bind - Secunia	af854a
The Slackware Linux Project: Slackware Security Advisories	af854a
www.freebsd.org/security/advisories/FreeBSD-SA-14:04.bind.asc	af854a
[SECURITY] Fedora 19 Update: bind-9.9.3-14.P2.fc19	af854a
Support / Security / Advisories / / MDVSA-2014:002 | Mandriva	af854a
CVE-2014-0591: A Crafted Query Against an NSEC3-signed Zone Can Crash BIND | Internet Systems Consortium Knowledge Base	af854a
NEOHAPSIS - Peace of Mind Through Integrity and Insight	af854a
openSUSE-SU-2014:0202-1: moderate: update for bind	af854a
[SECURITY] Fedora 20 Update: bind-9.9.4-11.P2.fc20	af854a
Security Advisory SA56574 - Red Hat update for bind - Secunia	af854a
Security Advisory SA61343 - Oracle Linux update for bind97 - Secunia	af854a
Security Advisory SA56522 - HP-UX BIND NSEC3-Signed Zones Queries Handling Denial of Service Vulnerability - Secunia	af854a
Security Advisory SA56427 - ISC BIND NSEC3-Signed Zones Queries Handling Denial of Service Vulnerability - Secunia	af854a
About Secunia Research | Flexera	af854a
CVE-2014-0591: FAQ and Supplemental Information | Internet Systems Consortium Knowledge Base	af854a
openSUSE-SU-2014:0199-1: moderate: update for bind	af854a
CVE Program record	CVE.C
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

15150 ISC BIND Crafted Query Vulnerability (CVE-2014-0591)

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**