



CVE-2015-4620

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2015-4620
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-08 14:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	name.c in named in ISC BIND 9.7.x through 9.9.x before 9.9.7-P1 and 9.10.x before 9.10.2-P2, when configured as a recur

Risk And Classification

Problem Types: CWE-17

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	isc	Bind	9.10.0	All	All	All
Application	isc	Bind	9.10.1	All	All	All
Application	isc	Bind	9.10.1	p1	All	All
Application	isc	Bind	9.10.2	b1	All	All
Application	isc	Bind	9.10.2	p1	All	All
Application	isc	Bind	9.10.2	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	lsc	Bind	9.7.2	p1	All	All
Application	lsc	Bind	9.7.2	p2	All	All
Application	lsc	Bind	9.7.2	p3	All	All
Application	lsc	Bind	9.7.2	rc1	All	All
Application	lsc	Bind	9.7.3	All	All	All
Application	lsc	Bind	9.7.3	b1	All	All
Application	lsc	Bind	9.7.3	p1	All	All
Application	lsc	Bind	9.7.3	rc1	All	All
Application	lsc	Bind	9.7.4	All	All	All
Application	lsc	Bind	9.7.4	b1	All	All
Application	lsc	Bind	9.7.4	p1	All	All
Application	lsc	Bind	9.7.4	rc1	All	All
Application	lsc	Bind	9.7.5	All	All	All
Application	lsc	Bind	9.7.5	b1	All	All
Application	lsc	Bind	9.7.5	rc1	All	All
Application	lsc	Bind	9.7.5	rc2	All	All
Application	lsc	Bind	9.7.6	All	All	All
Application	lsc	Bind	9.7.6	p1	All	All
Application	lsc	Bind	9.7.6	p2	All	All
Application	lsc	Bind	9.7.7	All	All	All
Application	lsc	Bind	9.8.0	All	All	All
Application	lsc	Bind	9.8.0	a1	All	All
Application	lsc	Bind	9.8.0	b1	All	All
Application	lsc	Bind	9.8.0	p1	All	All
Application	lsc	Bind	9.8.0	p2	All	All
Application	lsc	Bind	9.8.0	p4	All	All
Application	lsc	Bind	9.8.0	rc1	All	All
Application	lsc	Bind	9.8.1	All	All	All
Application	lsc	Bind	9.8.1	b1	All	All
Application	lsc	Bind	9.8.1	b2	All	All
Application	lsc	Bind	9.8.1	b3	All	All
Application	lsc	Bind	9.8.1	p1	All	All
Application	lsc	Bind	9.8.1	rc1	All	All
Application	lsc	Bind	9.8.2	b1	All	All
Application	lsc	Bind	9.8.2	rc1	All	All

Application	lsc	Bind	9.8.2	rc2	All	All
Application	lsc	Bind	9.8.3	All	All	All
Application	lsc	Bind	9.8.3	p1	All	All
Application	lsc	Bind	9.8.3	p2	All	All
Application	lsc	Bind	9.8.4	All	All	All
Application	lsc	Bind	9.8.5	All	All	All
Application	lsc	Bind	9.8.5	b1	All	All
Application	lsc	Bind	9.8.5	b2	All	All
Application	lsc	Bind	9.8.5	p1	All	All
Application	lsc	Bind	9.8.5	p2	All	All
Application	lsc	Bind	9.8.5	rc1	All	All
Application	lsc	Bind	9.8.5	rc2	All	All
Application	lsc	Bind	9.8.6	b1	All	All
Application	lsc	Bind	9.8.6	rc1	All	All
Application	lsc	Bind	9.8.6	rc2	All	All
Application	lsc	Bind	9.9.0	All	All	All
Application	lsc	Bind	9.9.0	a1	All	All
Application	lsc	Bind	9.9.0	a2	All	All
Application	lsc	Bind	9.9.0	a3	All	All
Application	lsc	Bind	9.9.0	b1	All	All
Application	lsc	Bind	9.9.0	b2	All	All
Application	lsc	Bind	9.9.0	rc1	All	All
Application	lsc	Bind	9.9.0	rc2	All	All
Application	lsc	Bind	9.9.0	rc3	All	All
Application	lsc	Bind	9.9.0	rc4	All	All
Application	lsc	Bind	9.9.1	All	All	All
Application	lsc	Bind	9.9.1	p1	All	All
Application	lsc	Bind	9.9.1	p2	All	All
Application	lsc	Bind	9.9.2	All	All	All
Application	lsc	Bind	9.9.3	All	All	All
Application	lsc	Bind	9.9.3	b1	All	All
Application	lsc	Bind	9.9.3	b2	All	All
Application	lsc	Bind	9.9.3	p1	All	All
Application	lsc	Bind	9.9.3	p2	All	All
Application	lsc	Bind	9.9.3	rc1	All	All
Application	lsc	Bind	9.9.3	rc2	All	All

Application	lsc	Bind	9.9.3	rc2	All	All
Application	lsc	Bind	9.9.4	b1	All	All
Application	lsc	Bind	9.9.5	All	All	All
Application	lsc	Bind	9.9.6	All	All	All
Application	lsc	Bind	9.9.6	p1	All	All
Application	lsc	Bind	9.9.7	b1	All	All
Application	lsc	Bind	9.9.7	rc1	All	All
Application	lsc	Bind	9.9.7	rc2	All	All
Application	lsc	Bind	9.10.0	All	All	All
Application	lsc	Bind	9.10.1	All	All	All
Application	lsc	Bind	9.10.1	p1	All	All
Application	lsc	Bind	9.10.2	b1	All	All
Application	lsc	Bind	9.10.2	p1	All	All
Application	lsc	Bind	9.10.2	rc1	All	All
Application	lsc	Bind	9.7.0	All	All	All
Application	lsc	Bind	9.7.0	b1	All	All
Application	lsc	Bind	9.7.0	p1	All	All
Application	lsc	Bind	9.7.0	p2	All	All
Application	lsc	Bind	9.7.0	rc1	All	All
Application	lsc	Bind	9.7.0	rc2	All	All
Application	lsc	Bind	9.7.1	All	All	All
Application	lsc	Bind	9.7.1	p1	All	All
Application	lsc	Bind	9.7.1	p2	All	All
Application	lsc	Bind	9.7.1	rc1	All	All
Application	lsc	Bind	9.7.2	All	All	All
Application	lsc	Bind	9.7.2	p1	All	All
Application	lsc	Bind	9.7.2	p2	All	All
Application	lsc	Bind	9.7.2	p3	All	All
Application	lsc	Bind	9.7.2	rc1	All	All
Application	lsc	Bind	9.7.3	All	All	All
Application	lsc	Bind	9.7.3	b1	All	All
Application	lsc	Bind	9.7.3	p1	All	All
Application	lsc	Bind	9.7.3	rc1	All	All
Application	lsc	Bind	9.7.4	All	All	All
Application	lsc	Bind	9.7.4	b1	All	All
Application	lsc	Bind	9.7.4	p1	All	All

Application	lsc	Bind	9.7.4	rc1	All	All
Application	lsc	Bind	9.7.5	All	All	All
Application	lsc	Bind	9.7.5	b1	All	All
Application	lsc	Bind	9.7.5	rc1	All	All
Application	lsc	Bind	9.7.5	rc2	All	All
Application	lsc	Bind	9.7.6	All	All	All
Application	lsc	Bind	9.7.6	p1	All	All
Application	lsc	Bind	9.7.6	p2	All	All
Application	lsc	Bind	9.7.7	All	All	All
Application	lsc	Bind	9.8.0	All	All	All
Application	lsc	Bind	9.8.0	a1	All	All
Application	lsc	Bind	9.8.0	b1	All	All
Application	lsc	Bind	9.8.0	p1	All	All
Application	lsc	Bind	9.8.0	p2	All	All
Application	lsc	Bind	9.8.0	p4	All	All
Application	lsc	Bind	9.8.0	rc1	All	All
Application	lsc	Bind	9.8.1	All	All	All
Application	lsc	Bind	9.8.1	b1	All	All
Application	lsc	Bind	9.8.1	b2	All	All
Application	lsc	Bind	9.8.1	b3	All	All
Application	lsc	Bind	9.8.1	p1	All	All
Application	lsc	Bind	9.8.1	rc1	All	All
Application	lsc	Bind	9.8.2	b1	All	All
Application	lsc	Bind	9.8.2	rc1	All	All
Application	lsc	Bind	9.8.2	rc2	All	All
Application	lsc	Bind	9.8.3	All	All	All
Application	lsc	Bind	9.8.3	p1	All	All
Application	lsc	Bind	9.8.3	p2	All	All
Application	lsc	Bind	9.8.4	All	All	All
Application	lsc	Bind	9.8.5	All	All	All
Application	lsc	Bind	9.8.5	b1	All	All
Application	lsc	Bind	9.8.5	b2	All	All
Application	lsc	Bind	9.8.5	p1	All	All
Application	lsc	Bind	9.8.5	p2	All	All
Application	lsc	Bind	9.8.5	rc1	All	All

Application	lsc	Bind	9.8.5	rc2	All	All
Application	lsc	Bind	9.8.6	b1	All	All
Application	lsc	Bind	9.8.6	rc1	All	All
Application	lsc	Bind	9.8.6	rc2	All	All
Application	lsc	Bind	9.9.0	All	All	All
Application	lsc	Bind	9.9.0	a1	All	All
Application	lsc	Bind	9.9.0	a2	All	All
Application	lsc	Bind	9.9.0	a3	All	All
Application	lsc	Bind	9.9.0	b1	All	All
Application	lsc	Bind	9.9.0	b2	All	All
Application	lsc	Bind	9.9.0	rc1	All	All
Application	lsc	Bind	9.9.0	rc2	All	All
Application	lsc	Bind	9.9.0	rc3	All	All
Application	lsc	Bind	9.9.0	rc4	All	All
Application	lsc	Bind	9.9.1	All	All	All
Application	lsc	Bind	9.9.1	p1	All	All
Application	lsc	Bind	9.9.1	p2	All	All
Application	lsc	Bind	9.9.2	All	All	All
Application	lsc	Bind	9.9.3	All	All	All
Application	lsc	Bind	9.9.3	b1	All	All
Application	lsc	Bind	9.9.3	b2	All	All
Application	lsc	Bind	9.9.3	p1	All	All
Application	lsc	Bind	9.9.3	p2	All	All
Application	lsc	Bind	9.9.3	rc1	All	All
Application	lsc	Bind	9.9.3	rc2	All	All
Application	lsc	Bind	9.9.4	b1	All	All
Application	lsc	Bind	9.9.5	All	All	All
Application	lsc	Bind	9.9.6	All	All	All
Application	lsc	Bind	9.9.6	p1	All	All
Application	lsc	Bind	9.9.7	b1	All	All
Application	lsc	Bind	9.9.7	rc1	All	All
Application	lsc	Bind	9.9.7	rc2	All	All

References
Reference
Red Hat Customer Portal

BIND 9.10.3 Release Notes Internet Systems Consortium Knowledge Base
404 Page not found
Debian -- Security Information -- DSA-3304-1 bind9
Red Hat Customer Portal
[SECURITY] Fedora 21 Update: bind-9.9.6-9.P1.fc21
McAfee KnowledgeBase - Intel Security - Security Bulletin: Firewall Enterprise update fixes CVE-2015-4620 (BIND) vulnerability
CVE-2015-4620 ISC Bind Vulnerability in NetApp Products NetApp Product Security
USN-2669-1: Bind vulnerability Ubuntu
ISC BIND DNSSEC Validation Flaw Lets Remote Users Deny Service in Certain Cases - SecurityTracker
2017-04 Security Bulletin: Multiple Vulnerabilities in NorthStar Controller Application before version 2.1.0 Service Pack 1. - Juniper Networks
CVE-2015-4620: Specially Constructed Zone Data Can Cause a Resolver to Crash when Validating Internet Systems Consortium Knowledge Base
[security-announce] SUSE-SU-2015:1205-1: important: Security update for openSUSE-SU-2015:1250-1: moderate: Security update for bind
BIND: Denial of Service (GLSA 201510-01) — Gentoo Security
ISC BIND 'isselfsigned()' Function Remote Denial of Service Vulnerability
[security-announce] openSUSE-SU-2015:1326-1: important: Security update
[SECURITY] Fedora 22 Update: bind-9.10.2-3.P2.fc22
BIND 9.9.8-S1 Release Notes Internet Systems Consortium Knowledge Base
BIND 9.9.8 Release Notes Internet Systems Consortium Knowledge Base
'[security bulletin] HPSBUX03379 SSRT101976 rev.1 - HP-UX Running BIND, Remote Denial of Service (DoS' - MARC
CVE Program record
NVD vulnerability detail
No vendor comments have been submitted for this CVE.
Legacy QID Mappings
15148 ISC BIND Denial of Service (DoS) Vulnerability (CVE-2015-4620)

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)