



CVE-2015-1349

Published on: 02/18/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:09 PM UTC

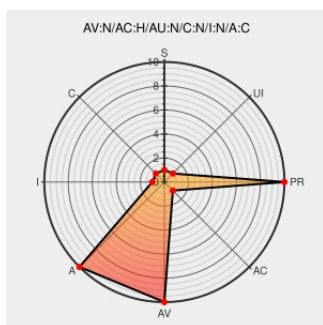
CVE-2015-1349

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Bind](#) from [Isc](#) contain the following vulnerability: named in ISC BIND 9.7.0 through 9.9.6 before 9.9.6-P2 and 9.10.x before 9.10.1-P2, when DNSSEC validation and the managed-keys feature are enabled, allows remote attackers to cause a denial of service (assertion failure and daemon exit, or daemon crash) by triggering an incorrect trust-anchor management scenario in which no key is ready for use.

CVE-2015-1349 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5.4 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

HIGH

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

COMPLETE

CVE References

Description

Tags

Link

McAfee KnowledgeBase - Intel Security - Security Bulletin: Patches resolve Firewall Enterprise vulnerabilities including CVE-2015-1349 (BIND)

kc.mcafee.com
text/html

CONFIRM
kc.mcafee.com/corporate/index?page=content&id=SB10116

About the security content of OS X Server v5.0.3 - Apple Support

support.apple.com
text/html

CONFIRM
support.apple.com/HT205219

1193820 - (CVE-2015-1349) CVE-2015-1349 bind: issue in trust anchor management can cause named to crash

bugzilla.redhat.com
text/html

CONFIRM
bugzilla.redhat.com/show_bug.cgi?id=1193820

[SECURITY] Fedora 21 Update: bind-9.9.6-8.P1.fc21

lists.fedoraproject.org
text/html

FEDORA **FEDORA-2015-2543**

2017-04 Security Bulletin: Multiple Vulnerabilities in NorthStar Controller

kb.juniper.net

CONFIRM

Application before version 2.1.0 Service Pack 1. - Juniper Networks	text/html	kb.juniper.net/JSA10/83
[security-announce] SUSE-SU-2015:1205-1: important: Security update for	lists.opensuse.org text/html	 SUSE SUSE-SU-2015:1205
openSUSE-SU-2015:1250-1: moderate: Security update for bind	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:1250
CVE-2015-1349: A Problem with Trust Anchor Management Can Cause named to Crash Internet Systems Consortium Knowledge Base	Vendor Advisory kb.isc.org text/html	 CONFIRM kb.isc.org/article/AA-01235
APPLE-SA-2015-09-16-4 OS X Server 5.0.3	lists.apple.com text/html	 APPLE APPLE-SA-2015-09-16-4
Support / Security / Advisories // MDVSA-2015:054 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2015:054
USN-2503-1: Bind vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-2503-1
BIND: Denial of Service (GLSA 201510-01) — Gentoo Security	security.gentoo.org text/html	 GENTOO GLSA-201510-01
[SECURITY] Fedora 20 Update: bind-9.9.4-18.P2.fc20	lists.fedoraproject.org text/html	 FEDORA FEDORA-2015-2548
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2015:0672
[security-announce] openSUSE-SU-2015:1326-1: important: Security update	lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:1326
Support / Security / Advisories // MDVSA-2015:165 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2015:165
'[security bulletin] HPSBUX03379 SSRT101976 rev.1 - HP-UX Running BIND, Remote Denial of Service (DoS' - MARC	marc.info text/html	 HP SSRT101976
Mageia Advisory: MGASA-2015-0082 - Updated bind packages fix CVE-2015-1349	advisories.mageia.org text/html	 CONFIRM advisories.mageia.org/MGASA-2015-0082.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[15149](#) ISC BIND Denial of Service (DoS) Vulnerability (CVE-2015-1349)

Known Affected Configurations (CPE V2.3)

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	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	Isc	Bind	9.9.0	rc4	All	All
Application	Isc	Bind	9.9.1	All	All	All
Application	Isc	Bind	9.9.1	p1	All	All
Application	Isc	Bind	9.9.1	p2	All	All
Application	Isc	Bind	9.9.2	All	All	All
Application	Isc	Bind	9.9.3	All	All	All
Application	Isc	Bind	9.9.3	b1	All	All
Application	Isc	Bind	9.9.3	b2	All	All
Application	Isc	Bind	9.9.3	p1	All	All
Application	Isc	Bind	9.9.3	p2	All	All
Application	Isc	Bind	9.9.3	rc1	All	All
Application	Isc	Bind	9.9.3	rc2	All	All
Application	Isc	Bind	9.9.4	b1	All	All
Application	Isc	Bind	9.9.5	All	All	All
Application	Isc	Bind	9.9.6	All	All	All
Application	Isc	Bind	9.9.6	p1	All	All
Application	Isc	Bind	9.9.7	b1	All	All
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	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	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	Isc	Bind	9.9.6	All	All	All
Application	Isc	Bind	9.9.6	p1	All	All
Application	Isc	Bind	9.9.7	b1	All	All
cpe:2.3:a:isc:bind:9.10.0:*****:						
cpe:2.3:a:isc:bind:9.10.1:*****:						
cpe:2.3:a:isc:bind:9.10.1:p1:*****:						
cpe:2.3:a:isc:bind:9.10.2:b1:*****:						
cpe:2.3:a:isc:bind:9.10.2:rc1:*****:						
cpe:2.3:a:isc:bind:9.7.0:*****:						
cpe:2.3:a:isc:bind:9.7.0:b1:*****:						
cpe:2.3:a:isc:bind:9.7.0:p1:*****:						
cpe:2.3:a:isc:bind:9.7.0:p2:*****:						
cpe:2.3:a:isc:bind:9.7.0:rc1:*****:						
cpe:2.3:a:isc:bind:9.7.0:rc2:*****:						
cpe:2.3:a:isc:bind:9.7.1:*****:						
cpe:2.3:a:isc:bind:9.7.1:p1:*****:						
cpe:2.3:a:isc:bind:9.7.1:p2:*****:						
cpe:2.3:a:isc:bind:9.7.1:rc1:*****:						
cpe:2.3:a:isc:bind:9.7.2:*****:						
cpe:2.3:a:isc:bind:9.7.2:p1:*****:						
cpe:2.3:a:isc:bind:9.7.2:p2:*****:						
cpe:2.3:a:isc:bind:9.7.2:p3:*****:						
cpe:2.3:a:isc:bind:9.7.2:rc1:*****:						
cpe:2.3:a:isc:bind:9.7.3:*****:						
cpe:2.3:a:isc:bind:9.7.3:b1:*****:						
cpe:2.3:a:isc:bind:9.7.3:p1:*****:						
cpe:2.3:a:isc:bind:9.7.3:rc1:*****:						
cpe:2.3:a:isc:bind:9.7.4:*****:						
cpe:2.3:a:isc:bind:9.7.4:b1:*****:						

cpe:2.3:a:isc:bind:9.7.4:p1:*****:
cpe:2.3:a:isc:bind:9.7.4:rc1:*****:
cpe:2.3:a:isc:bind:9.7.5:*****:
cpe:2.3:a:isc:bind:9.7.5:b1:*****:
cpe:2.3:a:isc:bind:9.7.5:rc1:*****:
cpe:2.3:a:isc:bind:9.7.5:rc2:*****:
cpe:2.3:a:isc:bind:9.7.6:*****:
cpe:2.3:a:isc:bind:9.7.6:p1:*****:
cpe:2.3:a:isc:bind:9.7.6:p2:*****:
cpe:2.3:a:isc:bind:9.7.7:*****:
cpe:2.3:a:isc:bind:9.8.0:*****:
cpe:2.3:a:isc:bind:9.8.0:a1:*****:
cpe:2.3:a:isc:bind:9.8.0:b1:*****:
cpe:2.3:a:isc:bind:9.8.0:p1:*****:
cpe:2.3:a:isc:bind:9.8.0:p2:*****:
cpe:2.3:a:isc:bind:9.8.0:p4:*****:
cpe:2.3:a:isc:bind:9.8.0:rc1:*****:
cpe:2.3:a:isc:bind:9.8.1:*****:
cpe:2.3:a:isc:bind:9.8.1:b1:*****:
cpe:2.3:a:isc:bind:9.8.1:b2:*****:
cpe:2.3:a:isc:bind:9.8.1:b3:*****:
cpe:2.3:a:isc:bind:9.8.1:p1:*****:
cpe:2.3:a:isc:bind:9.8.1:rc1:*****:
cpe:2.3:a:isc:bind:9.8.2:b1:*****:
cpe:2.3:a:isc:bind:9.8.2:rc1:*****:
cpe:2.3:a:isc:bind:9.8.2:rc2:*****:
cpe:2.3:a:isc:bind:9.8.3:*****:
cpe:2.3:a:isc:bind:9.8.3:p1:*****:
cpe:2.3:a:isc:bind:9.8.3:p2:*****:

676.2.0.α.136.0114.0.0.0.p2.

```
cpe:2.3:a:isc:bind:9.8.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:isc:bind:9.8.5:*:*:*:*:*:*:
```

```
cpe:2.3:a:isc:bind:9.8.5:b1:*.:*:*:*:*:
```

```
cpe:2.3:a:isc:bind:9.8.5:b2:*:*:*:*:*:
```

```
cpe:2.3:a:isc:bind:9.8.5:p1:*:*:*:*:*:
```

cpe:2.3:a:isc:bind:9.8.5:p2:*:*:*:*:*:

```
cpe:2.3:a:isc:bind:9.8.5:rc1:*:*:*:*:*:
```

cpe:2.3:a:isc:bind:9.8.5:rc2:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.8.6:b1:*:*:*:*:*:

```
cpe:2.3:a:isc:bind:9.8.6:rc1:*:*:*:*:*:
```

cpe:2.3:a:isc:bind:9.8.6:rc2:*:*:*:*:*:

```
cpe:2.3:a:isc:bind:9.9.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:isc:bind:9.9.0:a1:.*:.*:.*:.*:.*:.*
```

cpe:2.3:a:isc:bind:9.9.0:a2:*:*:*:*:*:

```
cpe:2.3:a:isc:bind:9.9.0:a3:*.:*:*:*:*:
```

cpe:2.3:a:isc:bind:9.9.0:b1:.*:.*:.*:.*:.*:.*

cpe:2.3:a:isc:bind:9.9.0:b2:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.9.0:rc1:*:*:*:*:*:

```
cpe:2.3:a:isc:bind:9.9.0:rc2:*:*:*:*:*:
```

cpe:2.3:a:isc:bind:9.9.0:rc3:*:*:*:*:*:

```
cpe:2.3:a:isc:bind:9.9.0:rc4:*:*:*:*:*:
```

```
cpe:2.3:a:isc:bind:9.9.1:.*:.*:.*:.*:.*:.*:.*
```

cpe:2.3:a:isc:bind:9.9.1:p1:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.9.1:p2:*:*:*:*:*:

```
cpe:2.3:a:isc:bind:9.9.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:isc:bind:9.9.3:*:*:*:*:*:*
```

```
cpe:2.3:a:isc:bind:9.9.3:b1:.*:.*:.*:.*:.*:.*
```

cpe:2.3:a:isc:bind:9.9.3:b2:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.9.3:p1:*****:
cpe:2.3:a:isc:bind:9.9.3:p2:*****:
cpe:2.3:a:isc:bind:9.9.3:rc1:*****:
cpe:2.3:a:isc:bind:9.9.3:rc2:*****:
cpe:2.3:a:isc:bind:9.9.4:b1:*****:
cpe:2.3:a:isc:bind:9.9.5:*****:
cpe:2.3:a:isc:bind:9.9.6:*****:
cpe:2.3:a:isc:bind:9.9.6:p1:*****:
cpe:2.3:a:isc:bind:9.9.7:b1:*****:
cpe:2.3:a:isc:bind:9.10.0:*****:
cpe:2.3:a:isc:bind:9.10.1:*****:
cpe:2.3:a:isc:bind:9.10.1:p1:*****:
cpe:2.3:a:isc:bind:9.10.2:b1:*****:
cpe:2.3:a:isc:bind:9.10.2:rc1:*****:
cpe:2.3:a:isc:bind:9.7.0:*****:
cpe:2.3:a:isc:bind:9.7.0:b1:*****:
cpe:2.3:a:isc:bind:9.7.0:p1:*****:
cpe:2.3:a:isc:bind:9.7.0:p2:*****:
cpe:2.3:a:isc:bind:9.7.0:rc1:*****:
cpe:2.3:a:isc:bind:9.7.0:rc2:*****:
cpe:2.3:a:isc:bind:9.7.1:*****:
cpe:2.3:a:isc:bind:9.7.1:p1:*****:
cpe:2.3:a:isc:bind:9.7.1:p2:*****:
cpe:2.3:a:isc:bind:9.7.1:rc1:*****:
cpe:2.3:a:isc:bind:9.7.2:*****:
cpe:2.3:a:isc:bind:9.7.2:p1:*****:
cpe:2.3:a:isc:bind:9.7.2:p2:*****:
cpe:2.3:a:isc:bind:9.7.2:p3:*****:

cpe:2.3:a:isc:bind:9.7.2:rc1:*****:
cpe:2.3:a:isc:bind:9.7.3:*****:
cpe:2.3:a:isc:bind:9.7.3:b1:*****:
cpe:2.3:a:isc:bind:9.7.3:p1:*****:
cpe:2.3:a:isc:bind:9.7.3:rc1:*****:
cpe:2.3:a:isc:bind:9.7.4:*****:
cpe:2.3:a:isc:bind:9.7.4:b1:*****:
cpe:2.3:a:isc:bind:9.7.4:p1:*****:
cpe:2.3:a:isc:bind:9.7.4:rc1:*****:
cpe:2.3:a:isc:bind:9.7.5:*****:
cpe:2.3:a:isc:bind:9.7.5:b1:*****:
cpe:2.3:a:isc:bind:9.7.5:rc1:*****:
cpe:2.3:a:isc:bind:9.7.5:rc2:*****:
cpe:2.3:a:isc:bind:9.7.6:*****:
cpe:2.3:a:isc:bind:9.7.6:p1:*****:
cpe:2.3:a:isc:bind:9.7.6:p2:*****:
cpe:2.3:a:isc:bind:9.7.7:*****:
cpe:2.3:a:isc:bind:9.8.0:*****:
cpe:2.3:a:isc:bind:9.8.0:a1:*****:
cpe:2.3:a:isc:bind:9.8.0:b1:*****:
cpe:2.3:a:isc:bind:9.8.0:p1:*****:
cpe:2.3:a:isc:bind:9.8.0:p2:*****:
cpe:2.3:a:isc:bind:9.8.0:p4:*****:
cpe:2.3:a:isc:bind:9.8.0:rc1:*****:
cpe:2.3:a:isc:bind:9.8.1:*****:
cpe:2.3:a:isc:bind:9.8.1:b1:*****:
cpe:2.3:a:isc:bind:9.8.1:b2:*****:
cpe:2.3:a:isc:bind:9.8.1:b3:*****:
cpe:2.3:a:isc:bind:9.8.1:p1:*****:

cpe:2.3:a:isc:bind:9.8.1:rc1:*****:
cpe:2.3:a:isc:bind:9.8.2:b1:*****:
cpe:2.3:a:isc:bind:9.8.2:rc1:*****:
cpe:2.3:a:isc:bind:9.8.2:rc2:*****:
cpe:2.3:a:isc:bind:9.8.3:*****:
cpe:2.3:a:isc:bind:9.8.3:p1:*****:
cpe:2.3:a:isc:bind:9.8.3:p2:*****:
cpe:2.3:a:isc:bind:9.8.4:*****:
cpe:2.3:a:isc:bind:9.8.5:*****:
cpe:2.3:a:isc:bind:9.8.5:b1:*****:
cpe:2.3:a:isc:bind:9.8.5:b2:*****:
cpe:2.3:a:isc:bind:9.8.5:p1:*****:
cpe:2.3:a:isc:bind:9.8.5:p2:*****:
cpe:2.3:a:isc:bind:9.8.5:rc1:*****:
cpe:2.3:a:isc:bind:9.8.5:rc2:*****:
cpe:2.3:a:isc:bind:9.8.6:b1:*****:
cpe:2.3:a:isc:bind:9.8.6:rc1:*****:
cpe:2.3:a:isc:bind:9.8.6:rc2:*****:
cpe:2.3:a:isc:bind:9.9.0:*****:
cpe:2.3:a:isc:bind:9.9.0:a1:*****:
cpe:2.3:a:isc:bind:9.9.0:a2:*****:
cpe:2.3:a:isc:bind:9.9.0:a3:*****:
cpe:2.3:a:isc:bind:9.9.0:b1:*****:
cpe:2.3:a:isc:bind:9.9.0:b2:*****:
cpe:2.3:a:isc:bind:9.9.0:rc1:*****:
cpe:2.3:a:isc:bind:9.9.0:rc2:*****:
cpe:2.3:a:isc:bind:9.9.0:rc3:*****:
cpe:2.3:a:isc:bind:9.9.0:rc4:*****:

cpe:2.3:a:isc:bind:9.9.1:*****:
cpe:2.3:a:isc:bind:9.9.1:p1:*****:
cpe:2.3:a:isc:bind:9.9.1:p2:*****:
cpe:2.3:a:isc:bind:9.9.2:*****:
cpe:2.3:a:isc:bind:9.9.3:*****:
cpe:2.3:a:isc:bind:9.9.3:b1:*****:
cpe:2.3:a:isc:bind:9.9.3:b2:*****:
cpe:2.3:a:isc:bind:9.9.3:p1:*****:
cpe:2.3:a:isc:bind:9.9.3:p2:*****:
cpe:2.3:a:isc:bind:9.9.3:rc1:*****:
cpe:2.3:a:isc:bind:9.9.3:rc2:*****:
cpe:2.3:a:isc:bind:9.9.4:b1:*****:
cpe:2.3:a:isc:bind:9.9.5:*****:
cpe:2.3:a:isc:bind:9.9.6:*****:
cpe:2.3:a:isc:bind:9.9.6:p1:*****:
cpe:2.3:a:isc:bind:9.9.7:b1:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)