



# CVE-2013-2266

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

## Summary

<b>CVE</b>	CVE-2013-2266
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2013-03-28 16:55:00 UTC
<b>Updated</b>	2018-10-30 16:27:00 UTC
<b>Description</b>	libdns in ISC BIND 9.7.x and 9.8.x before 9.8.4-P2, 9.8.5 before 9.8.5b2, 9.9.x before 9.9.2-P2, and 9.9.3 before 9.9.3b2 or

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
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	9.7.3	All	All	All
Application	isc	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	9.8.0	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	9.9.0	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	9.7.0	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	9.8.0	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	9.9.0	All	All	All
Application	lsc	Bind	9.9.0	a1	All	All
Application	lsc	Bind	9.9.0	a2	All	All

Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.0	a3	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.0	b1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.0	b2	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.0	rc1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.0	rc2	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.0	rc3	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.0	rc4	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.1	All	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.1	p1	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.1	p2	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.2	All	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.3	All	All	All
Application	<a href="#">lsc</a>	<a href="#">Bind</a>	9.9.3	b1	All	All

## References

### Reference

[Red Hat Customer Portal](#)

[CVE-2013-2266: FAQ and Supplemental Information | Internet Systems Consortium Knowledge Base](#)

[Debian -- Security Information -- DSA-2656-1 bind9](#)

[APPLE-SA-2013-09-12-1 OS X Mountain Lion v10.8.5 and Security Update 2013-004](#)

[ISC BIND 9 'libdns' Remote Denial of Service Vulnerability](#)

[A Maliciously Crafted Regular Expression Can Cause Memory Exhaustion in named | Internet Systems Consortium](#)

[Repository / Oval Repository](#)

[About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004](#)

[Red Hat Customer Portal](#)

['\[security bulletin\] HPSBUX02876 SSRT101148 rev.1 - HP-UX Running BIND, Remote Denial of Service \(DoS\) - MARC](#)

[\[SECURITY\] Fedora 17 Update: bind-9.9.2-7.P2.fc17](#)

[USN-1783-1: Bind vulnerability | Ubuntu](#)

[\[SECURITY\] Fedora 18 Update: bind-9.9.2-10.P2.fc18](#)

404 Not Found

[CVE-2013-2266: A Maliciously Crafted Regular Expression Can Cause Memory Exhaustion in named | Internet Systems Consortium Knowled](#)

[CVE Program record](#)

[NVD vulnerability detail](#)

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#)