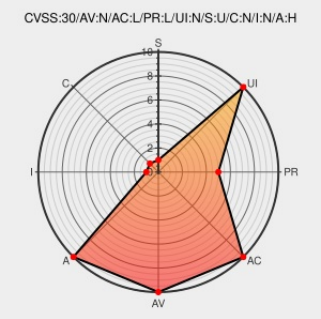
CVE-2015-8704

Published on: 01/20/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:13 PM UTC

CVE-2015-8704

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Bind from Isc contain the following vulnerability:

apl_42.c in ISC BIND 9.x before 9.9.8-P3, 9.9.x, and 9.10.x before 9.10.3-P3 allows remote authenticated users to cause a denial of service (INSIST assertion failure and daemon exit) via a malformed Address Prefix List (APL) record.

CVE-2015-8704 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.5 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 6.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	COMPLETE

CVE References

Description	Tags	Link
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2016:0073
Red Hat Customer Portal	web.archive.org	REDHAT RHSA-2016:0074

	text/html Inactive Link Not Archived	
404 Page not found	kb.isc.org text/html Inactive Link Not Archived	CONFIRM kb.isc.org/article/AA-01438
ISC BIND Overflow in Processing Address Prefix List Data Lets Remote Authenticated Users Cause the Target Service to Crash - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1034739
[security-announce] openSUSE-SU-2016:0197-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0197
[SECURITY] Fedora 22 Update: bind-9.10.3-8.P3.fc22	lists.fedoraproject.org text/html	FEDORA FEDORA-2016-1ab53bf440
[security-announce] openSUSE-SU-2016:0199-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0199
[security-announce] SUSE-SU-2016:0200-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0200
[SECURITY] Fedora 22 Update: bind99-9.9.8-2.P3.fc22	lists.fedoraproject.org text/html	FEDORA FEDORA-2016-1323b9078a
ISC BIND CVE-2015-8704 Remote Denial of Service Vulnerability	cve.report (archive) text/html	BID 81329
[security-announce] SUSE-SU-2016:0174-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0174
[security-announce] openSUSE-SU-2016:0204-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2016:0204
CVE-2015-8704: Specific APL data could trigger an INSIST in apl_42.c | Internet Systems Consortium Knowledge Base	Vendor Advisory kb.isc.org text/html	CONFIRM kb.isc.org/article/AA-01335
[SECURITY] Fedora 23 Update: bind99-9.9.8-2.P3.fc23	lists.fedoraproject.org text/html	FEDORA FEDORA-2016-feb8d77f36
[security-announce] SUSE-SU-2016:0227-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0227
'[security bulletin] HPSBUX03552 SSRT102983 rev.1 - HP-UX BIND running Named, Remote Denial of Servic' - MARC	Third Party Advisory marc.info text/html	HP SSRT102983
Oracle VM Server for x86 Bulletin - July 2016	web.archive.org text/html Inactive Link Not Archived	CONFIRM www.oracle.com/technetwork/topics/security/ovmbulletinjul2016-3090546.html
BIND 9.10.4 Release Notes | Internet Systems Consortium Knowledge Base	Vendor Advisory web.archive.org text/html Inactive Link Not Archived	CONFIRM kb.isc.org/article/AA-01380
	www.freebsd.org text/plain	FREEBSD FreeBSD-SA-16:08
USN-2874-1: Bind vulnerability | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-2874-1
[SECURITY] Fedora 23 Update: bind-9.10.3-10.P3.fc23	lists.fedoraproject.org text/html	FEDORA FEDORA-2016-f3517b9c4c
Oracle Linux Bulletin - January 2016	www.oracle.com	CONFIRM

Oracle Linux Bulletin - January 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
Debian -- Security Information -- DSA-3449-1 bind9	www.debian.org Depreciated Link text/html	DEBIAN DSA-3449
BIND: Multiple vulnerabilities (GLSA 201610-07) — Gentoo Security	security.gentoo.org text/html	GENTOO GLSA-201610-07
Oracle Solaris Bulletin - October 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletinoct2016-3090566.html
[security-announce] SUSE-SU-2016:0180-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2016:0180
Oracle Solaris Bulletin - January 2016	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/bulletinjan2016-2867206.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Isc	Bind	9.0	All	All	All
Application	Isc	Bind	9.0.1	All	All	All
Application	Isc	Bind	9.1	All	All	All
Application	Isc	Bind	9.1.1	All	All	All
Application	Isc	Bind	9.1.2	All	All	All
Application	Isc	Bind	9.1.3	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	All	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	p2	All	All
Application	Isc	Bind	9.10.2	p3	All	All
Application	Isc	Bind	9.10.2	p4	All	All
Application	Isc	Bind	9.10.2	rc1	All	All
Application	Isc	Bind	9.10.3	All	All	All
Application	Isc	Bind	9.10.3	p1	All	All

Application	Isc	Bind	9.10.3	p2	All	All
Application	Isc	Bind	9.10.3	rc1	All	All
Application	Isc	Bind	9.2	All	All	All
Application	Isc	Bind	9.2.0	All	All	All
Application	Isc	Bind	9.2.1	All	All	All
Application	Isc	Bind	9.2.2	All	All	All
Application	Isc	Bind	9.2.2	p3	All	All
Application	Isc	Bind	9.2.3	All	All	All
Application	Isc	Bind	9.2.4	All	All	All
Application	Isc	Bind	9.2.5	All	All	All
Application	Isc	Bind	9.2.6	All	All	All
Application	Isc	Bind	9.2.7	All	All	All
Application	Isc	Bind	9.3	All	All	All
Application	Isc	Bind	9.3.0	All	All	All
Application	Isc	Bind	9.3.1	All	All	All
Application	Isc	Bind	9.3.2	All	All	All
Application	Isc	Bind	9.3.3	All	All	All
Application	Isc	Bind	9.4	All	All	All
Application	Isc	Bind	9.4.0	All	All	All
Application	Isc	Bind	9.4.0	rc1	All	All
Application	Isc	Bind	9.4.1	All	All	All
Application	Isc	Bind	9.4.2	All	All	All
Application	Isc	Bind	9.4.3	All	All	All
Application	Isc	Bind	9.4.3	rc1	All	All
Application	Isc	Bind	9.5	All	All	All
Application	Isc	Bind	9.5.0	All	All	All
Application	Isc	Bind	9.5.0	rc1	All	All
Application	Isc	Bind	9.5.1	All	All	All
Application	Isc	Bind	9.5.1	rc1	All	All
Application	Isc	Bind	9.5.1	rc2	All	All
Application	Isc	Bind	9.5.2	All	All	All
Application	Isc	Bind	9.5.2	rc1	All	All
Application	Isc	Bind	9.5.3	All	All	All
Application	Isc	Bind	9.5.3	rc1	All	All
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	9.9.8	p2	All	All
Application	Isc	Bind	9.0	All	All	All
Application	Isc	Bind	9.0.1	All	All	All
Application	Isc	Bind	9.1	All	All	All
Application	Isc	Bind	9.1.1	All	All	All
Application	Isc	Bind	9.1.2	All	All	All
Application	Isc	Bind	9.1.3	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	All	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	p2	All	All
Application	Isc	Bind	9.10.2	p3	All	All
Application	Isc	Bind	9.10.2	p4	All	All
Application	Isc	Bind	9.10.2	rc1	All	All
Application	Isc	Bind	9.10.3	All	All	All
Application	Isc	Bind	9.10.3	p1	All	All
Application	Isc	Bind	9.10.3	p2	All	All
Application	Isc	Bind	9.10.3	rc1	All	All
Application	Isc	Bind	9.2	All	All	All
Application	Isc	Bind	9.2.0	All	All	All
Application	Isc	Bind	9.2.1	All	All	All
Application	Isc	Bind	9.2.2	All	All	All
Application	Isc	Bind	9.2.2	p3	All	All
Application	Isc	Bind	9.2.3	All	All	All
Application	Isc	Bind	9.2.4	All	All	All
Application	Isc	Bind	9.2.5	All	All	All
Application	Isc	Bind	9.2.6	All	All	All

Application	Isc	Bind	9.2.7	All	All	All
Application	Isc	Bind	9.3	All	All	All
Application	Isc	Bind	9.3.0	All	All	All
Application	Isc	Bind	9.3.1	All	All	All
Application	Isc	Bind	9.3.2	All	All	All
Application	Isc	Bind	9.3.3	All	All	All
Application	Isc	Bind	9.4	All	All	All
Application	Isc	Bind	9.4.0	All	All	All
Application	Isc	Bind	9.4.0	rc1	All	All
Application	Isc	Bind	9.4.1	All	All	All
Application	Isc	Bind	9.4.2	All	All	All
Application	Isc	Bind	9.4.3	All	All	All
Application	Isc	Bind	9.4.3	rc1	All	All
Application	Isc	Bind	9.5	All	All	All
Application	Isc	Bind	9.5.0	All	All	All
Application	Isc	Bind	9.5.0	rc1	All	All
Application	Isc	Bind	9.5.1	All	All	All
Application	Isc	Bind	9.5.1	rc1	All	All
Application	Isc	Bind	9.5.1	rc2	All	All
Application	Isc	Bind	9.5.2	All	All	All
Application	Isc	Bind	9.5.2	rc1	All	All
Application	Isc	Bind	9.5.3	All	All	All
Application	Isc	Bind	9.5.3	rc1	All	All
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	9.9.8	p2	All	All

cpe:2.3:a:isc:bind:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.1.3:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.2:b1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.2:p1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.2:p2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.2:p3:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.2:p4:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.3:p1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.3:p2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.3:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.2:p3:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.3:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.1:rc2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.3:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:r5_p1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:r6_b1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:r6_rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:r6_rc2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:r7_p1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:r7_p2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.9.8:p2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.1.3:*:*:*:*:*:*:*:

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:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.2:b1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.2:p1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.2:p2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.2:p3:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.2:p4:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.3:p1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.3:p2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.3:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.2:p3:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.4.3:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.0:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.1:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.1:rc2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.2:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.2:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.3:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.5.3:rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:r5_p1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:r6_b1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:r6_rc1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:r6_rc2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:r7_p1:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.6:r7_p2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.8:p2:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.9.8:p2:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→