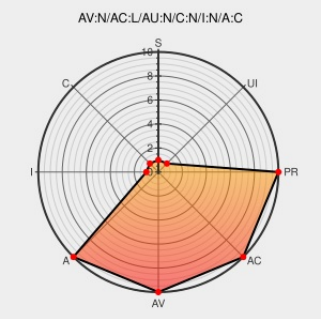
CVE-2012-5688

Published on: 12/06/2012 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:21 PM UTC

CVE-2012-5688

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

ISC BIND 9.8.x before 9.8.4-P1 and 9.9.x before 9.9.2-P1, when DNS64 is enabled, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.

CVE-2012-5688 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
Red Hat Customer Portal	Third Party Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2012:1549
USN-1657-1: Bind vulnerability | Ubuntu	Third Party Advisory, www.ubuntu.com, text/html	UBUNTU USN-1657-1
APPLE-SA-2013-09-12-1 OS X Mountain Lion v10.8.5 and Security Update 2013-004	Mailing List, Third Party Advisory, lists.apple.com, text/html	APPLE APPLE-SA-2013-09-12-1
The Slackware Linux Project: Slackware Security Advisories	Third Party Advisory, www.slackware.com, text/html	SLACKWARE SSA:2012-341-01

About the security content of OS X Mountain Lion v10.8.5 and Security Update 2013-004	Third Party Advisory support.apple.com text/html	CONFIRM support.apple.com/kb/HT5880
CVE-2012-5688: BIND 9 servers using DNS64 can be crashed by a crafted query | Internet Systems Consortium Knowledge Base	Patch Vendor Advisory kb.isc.org text/html	CONFIRM kb.isc.org/article/AA-00828

Related QID Numbers

690280 Free Berkeley Software Distribution (FreeBSD) Security Update for dns/bind9* (2892a8e2-3d68-11e2-8e01-0800273fe665)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Application	Isc	Bind	9.8.0	-	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
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	-	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
Application	Isc	Bind	9.8.3	p1	All	All
Application	Isc	Bind	9.8.3	p2	All	All
Application	Isc	Bind	9.8.3	p3	All	All
Application	Isc	Bind	9.8.3	p4	All	All
Application	Isc	Bind	9.9.0	-	All	All
Application	Isc	Bind	9.9.0	a1	All	All
Application	Isc	Bind	9.9.0	a2	All	All
Application	Isc	Bind	9.9.0	a3	All	All
Application	Isc	Bind	9.9.0	b1	All	All
Application	Isc	Bind	9.9.0	b2	All	All
Application	Isc	Bind	9.9.0	rc1	All	All
Application	Isc	Bind	9.9.0	rc2	All	All
Application	Isc	Bind	9.9.0	rc3	All	All
Application	Isc	Bind	9.9.0	rc4	All	All
Application	Isc	Bind	9.9.1	-	All	All
Application	Isc	Bind	9.9.1	p1	All	All
Application	Isc	Bind	9.9.1	p2	All	All
Application	Isc	Bind	9.9.1	p3	All	All
Application	Isc	Bind	9.9.1	p4	All	All
Application	Isc	Bind	9.8.0	-	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
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	-	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
Application	Isc	Bind	9.8.3	p1	All	All
Application	Isc	Bind	9.8.3	p2	All	All
Application	Isc	Bind	9.8.3	p3	All	All
Application	Isc	Bind	9.8.3	p4	All	All
Application	Isc	Bind	9.9.0	-	All	All
Application	Isc	Bind	9.9.0	a1	All	All
Application	Isc	Bind	9.9.0	a2	All	All
Application	Isc	Bind	9.9.0	a3	All	All
Application	Isc	Bind	9.9.0	b1	All	All
Application	Isc	Bind	9.9.0	b2	All	All
Application	Isc	Bind	9.9.0	rc1	All	All
Application	Isc	Bind	9.9.0	rc2	All	All
Application	Isc	Bind	9.9.0	rc3	All	All
Application	Isc	Bind	9.9.0	rc4	All	All
Application	Isc	Bind	9.9.1	-	All	All
Application	Isc	Bind	9.9.1	p1	All	All
Application	Isc	Bind	9.9.1	p2	All	All
Application	Isc	Bind	9.9.1	p3	All	All
Application	Isc	Bind	9.9.1	p4	All	All

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

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:-:*:*:*:*:*:*:

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:9.8.3:p3:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.8.3:p4:*:*:*:*:*:*:

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:9.9.1:p3:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.9.1:p4:*:*:*:*:*:*:

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:-:*:*:*:*:*:*:

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:9.8.3:p3:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.8.3:p4:*:*:*:*:*:*:

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:9.9.1:p3:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.9.1:p4:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→