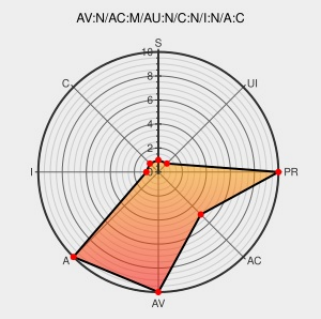
CVE-2012-5689

Published on: 01/25/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:20 PM UTC

CVE-2012-5689

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



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

ISC BIND 9.8.x through 9.8.4-P1 and 9.9.x through 9.9.2-P1, in certain configurations involving DNS64 with a Response Policy Zone that lacks an AAAA rewrite rule, allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query for an AAAA record.

CVE-2012-5689 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.1 - HIGH

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

CVE References

Description	Tags	Link
BIND 9 with DNS64 enabled can unexpectedly terminate when resolving domains in RPZ | Internet Systems Consortium	Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	CONFIRM www.isc.org/software/bind/advisories/cve-2012-5689
Red Hat Customer Portal	Third Party Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2013:0550
USN-2693-1: Bind vulnerabilities | Ubuntu	Third Party Advisory, www.ubuntu.com, text/html	UBUNTU USN-2693-1
CVE-2012-5689: BIND 9 with DNS64 enabled can unexpectedly	Vendor Advisory	CONFIRM kb.isc.org/article/AA-00855/

terminate when resolving domains in RPZ | Internet Systems Consortium Knowledge Base

kb.isc.org
text/html

There are currently no QIDs associated with this CVE

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	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Application	Isc	Bind	9.8.0	All	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	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	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	All

Application	Isc	Bind	9.8.3	p1	All	All
Application	Isc	Bind	9.8.3	p2	All	All
Application	Isc	Bind	9.8.4	All	All	All
Application	Isc	Bind	9.9.0	All	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	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	9.8.0	All	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	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	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	All
Application	Isc	Bind	9.8.3	p1	All	All

Application	Isc	Bind	9.8.3	p2	All	All
Application	Isc	Bind	9.8.4	All	All	All
Application	Isc	Bind	9.9.0	All	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	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
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.4.z	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.4.z	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

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

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:

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

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:

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:9.9.0:*:*:*:*:*:*:*:

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:9.8.0:*:*:*:*:*:*:*:

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:9.9.0:*:*:*:*:*:*:

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:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_hpc_node:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_hpc_node:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:6.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:6.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:6.4.z:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_eus:6.4.z:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report