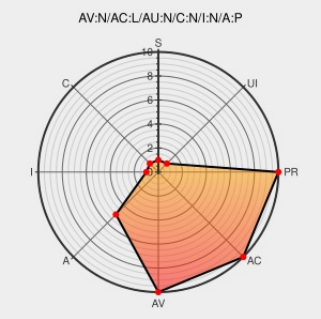
CVE-2014-3214

Published on: 05/08/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:46 PM UTC

CVE-2014-3214

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



Certain versions of Bind from Isc contain the following vulnerability:

The prefetch implementation in named in ISC BIND 9.10.0, when a recursive nameserver is enabled, allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a DNS query that triggers a response with unspecified attributes.

CVE-2014-3214 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

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

CVE References

Description	Tags	Link
CVE-2014-3214: A Defect in Prefetch Can Cause Recursive Servers to Crash | Internet Systems Consortium Knowledge Base	Vendor Advisory, kb.isc.org, text/html	CONFIRM kb.isc.org/article/AA-01161
ISC BIND Prefetch Bug Lets Remote Users Deny Service Against Recursive Nameservers - SecurityTracker	Third Party Advisory, VDB Entry, www.securitytracker.com, text/html	SECTRACK 1030214
BIND: Multiple Vulnerabilities (GLSA 201502-03) — Gentoo security	Third Party Advisory, VDB Entry, security.gentoo.org, text/html	GENTOO GLSA-201502-03

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.

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	9.10.0	All	All	All
Application	Isc	Bind	9.10.0	All	All	All

cpe:2.3:a:isc:bind:9.10.0:*:*:*:*:*:*:*:

cpe:2.3:a:isc:bind:9.10.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→