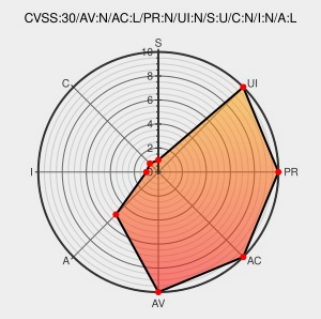
CVE-2019-6468

Published on: 10/09/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:01 PM UTC

CVE-2019-6468

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



Certain versions of Bind from Isc contain the following vulnerability:

In BIND Supported Preview Edition, an error in the nxdomain-redirect feature can occur in versions which support EDNS Client Subnet (ECS) features. In those versions which have ECS support, enabling nxdomain-redirect is likely to lead to BIND exiting due to assertion failure. Versions affected: BIND Supported Preview Edition version 9.10.5-S1 -> 9.11.5-S5. ONLY BIND Supported Preview Edition releases are affected.

CVE-2019-6468 has been assigned by security-officer@isc.org to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **ISC** - **BIND 9 Supported Preview Edition** version **9.10.5-S1 -> 9.11.5-S5**

Vulnerability Patch/Work Around

Exploitation of this defect can be effectively prevented by disabling the nxdomain-redirect feature in the nameserver's configuration.

CVSS3 Score: 7.5 - HIGH

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

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-2019-6468: BIND Supported Preview Edition can exit with an assertion failure if nxdomain-redirect is used - Security Advisories	Third Party Advisory kb.isc.org text/html	CONFIRM kb.isc.org/docs/cve-2019-6468
Synology Inc.	www.synology.com text/html	Syno CONFIRM www.synology.com/security/advisory/Synology_SA_19_20

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that 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	9.10.5	s1	All	All
Application	Isc	Bind	9.11.5	s5	All	All
Application	Isc	Bind	9.10.5	s1	All	All
Application	Isc	Bind	9.11.5	s5	All	All

cpe:2.3:a:isc:bind:9.10.5:s1:*:*:supported_preview:*:*:*:

cpe:2.3:a:isc:bind:9.11.5:s5:*:*:supported_preview:*:*:*:

cpe:2.3:a:isc:bind:9.10.5:s1:*:*:supported_preview:*:*:*:

cpe:2.3:a:isc:bind:9.11.5:s5:*:*:supported_preview:*:*:*:

Discovery Credit

ISC would like to thank Quad9 for reporting this issue.

← Previous ID

Next ID→