Search CTRL+K

About ISC
BIND 9
Security Advisories
BIND 9 Software Vulne...
List of BIND Security A...
ISC CVSS Scoring Guid...
2026
2025
2024
2023
2022
2021
Obsolete Matrices
Obsolete Branches
Operational Notifications
Significant changes
Navigating BIND docume...
Support and Contributing
Basics
Installation
Host platform issues
Networking and transports
DNS structure, protocol, a...
Control and protection wit...
Forwarders
Zones
Cache
Views

BIND 9 Software Vulnerability Matrix

TAGS

bind 9 | BIND 9-S | security | Security Vulnerability Matrix | vulnerability

IN THIS ARTICLE

Using this matrix
Determining vulnerability
Supported Preview Edition
Other BIND versions
The matrix

U 3 minute(s) read Focus Listen

FOLLOW

The BIND 9 Software Vulnerability Matrix details known security vulnerabilities in supported versions of BIND. Vulnerabilities are identified by their CVE ID: Common Vulnerability

Cookie consent

We use our own and third-party cookies to understand how you interact with our Knowledgebase. This helps us show you more relevant content and ads based on your browsing and navigation history.

Accept necessary cookies

dExposures.

This page was previously called the "BIND9 Security Vulnerability Matrix".

Using this matrix

Each row with a CVE ID gives the version(s) that fix that problem.

Determining vulnerability

Cookie consent

We use our own and third-party cookies to understand how you interact with our Knowledgebase. This helps us show you more relevant content and ads based on your browsing and navigation history.

determine if/how **giving version** is vulnerable:

- Find the column heading for the corresponding branch (9.X version)
- Read down that column to find the specific 9.X.Y version (or use "Find" in your browser)

To determine

Cookie consent

We use our own and third-party cookies to understand how you interact with our Knowledgebase. This helps us show you more relevant content and ads based on your browsing and navigation history.

Given CVE applies:

- Read down the "CVE ID" column to find the CVE ID (or use "Find" in your browser)
- If you do not know the CVE ID, consult the complete list of all INDadvisories

Once you find a given table row (CVE ID and/or

Cookie consent

We use our own and third-party cookies to understand how you interact with our Knowledgebase. This helps us show you more relevant content and ads based on your browsing and navigation history.

on):

- The listed version(s) contain fixes for that CVE, and are **not** vulnerable to that CVE
- A dash (-) indicates no version of that branch (column) is vulnerable to that CVE (row)
- That version **is** vulnerable to that CVE, and no later version of that branch (column) contains a fix for that CVE (row)

Cookie consent

We use our own and third-party cookies to understand how you interact with our Knowledgebase. This helps us show you more relevant content and ads based on your browsing and navigation history.

(above the row)
- That version is **not** vulnerable to earlier CVEs (below the row)

For table rows without a CVE:

- Add a dash (-) indicate that the row does not apply to that branch (column)

Supported Preview Edition

t CVE applyequallytoboththeopensourceeditionandtheSupportedPreviewEdition(-S).

- If a row lists the -S1 suffix, the CVE applies **only** to the Supported Preview Edition.
- If no -S1 suffix is present, the CVE

Cookie consent

We use our own and third-party cookies to understand how you interact with our Knowledgebase. This helps us show you more relevant content and ads based on your browsing and navigation history.

istoboththeditions.

Other BLND Versions

The major branches on this page will always reflect the currently-supported stable branch(es) of BLND. See [ISC's Software Support Policy and Version Numbering](). Older branch

IN Arenolongersupported.generallydonotreceivefixes.andmaynotevenbeassessedforvulnerability.Forhistoricalreference.Pleaseseematricesforrobsoletebranches.

Development.alpha.beta.orreleasecandidate(RC)v

nsare not listed here. We recommend that you use only stable branches in any environment for which security is a concern.

The matrix

Each row with a CVE ID gives the version(s) that fix that problem.

Cookie consent

We use our own and third-party cookies to understand how you interact with our Knowledgebase. This helps us show you more relevant content and ads based on your browsing and navigation history.

Cookie consent

We use our own and third-party cookies to understand how you interact with our Knowledgebase. This helps us show you more relevant content and ads based on your browsing and navigation history.

Related articles

Cookie consent

We use our own and third-party cookies to understand how you interact with our Knowledgebase. This helps us show you more relevant content and ads based on your browsing and navigation history.