Table of Contents

CVE-2023-5517: Querying RFC 1918 reverse zones may cause an assertion failure when nxdomain-redirect is enabled

CVE: CVE-2023-5517

Title: Querying RFC 1918 reverse zones may cause an assertion failure when "nxdomain-redirect" is enabled

Document version: 2.0

Posting date: 13 February 2024

Program impacted: BIND 9

Versions affected:

BIND

- 9.12.0 -> 9.16.45
- 9.18.0 -> 9.18.21
- 9.19.0 -> 9.19.19

BIND Supported Preview Edition

- 9.16.8-S1 -> 9.16.45-S1
- 9.18.11-S1 -> 9.18.21-S1

Severity: High

Exploitable: Remotely

Description:

A flaw in query-handling code can cause `named` to exit prematurely with an assertion failure when:

- `nxdomain-redirect <domain>;` is configured, and
- the resolver receives a PTR query for an RFC 1918 address that would normally result in an authoritative NXDOMAIN response.

Impact:

If both of the above conditions are met, a single suitable query will cause `named` to crash.

CVSS Score: 7.5

CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

For more information on the Common Vulnerability Scoring System and to obtain your specific environmental score please visit: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H&version=3.1.

Workarounds:

Disabling the `nxdomain-redirect` feature makes the faulty code path impossible to reach, preventing this flaw from being exploitable.

Active exploits:

We are not aware of any active exploits.

Solution:

Upgrade to the patched release most closely related to your current version of BIND 9:

- 9.16.48
- 9.18.24
- 9.19.21

BIND Supported Preview Edition is a special feature preview branch of BIND provided to eligible ISC support customers.

- 9.16.48-S1
- 9.18.24-S1

Document revision history:

- 1.0 Early Notification, 10 January 2024
- 1.1 Revised Early Notification, 15 January 2024
- 1.2 Revised the list of fixed versions, 11 February 2024
- 2.0 Public disclosure, 13 February 2024

Related documents:

See our BIND 9 Security Vulnerability Matrix for a complete listing of security vulnerabilities and versions affected.

Do you still have questions? Questions regarding this advisory should be mailed to bind-security@isc.org or posted as confidential GitLab issues at https://gitlab.isc.org/isc-projects/bind9/-/issues/new?issue[confidential]=true.

Note:

ISC patches only currently supported versions. When possible we indicate EOL versions affected. For current information on which versions are actively supported, please see https://www.isc.org/download/.

ISC Security Vulnerability Disclosure Policy:

Details of our current security advisory policy and practice can be found in the ISC Software Defect and Security Vulnerability Disclosure Policy at https://kb.isc.org/docs/aa-00861.

The Knowledgebase article https://kb.isc.org/docs/cve-2023-5517 is the complete and official security advisory document.

Legal Disclaimer: