Table of Contents

CVE-2023-50868: Preparing an NSEC3 closest encloser proof can exhaust CPU resources

CVE: CVE-2023-50868

Title: Preparing an NSEC3 closest encloser proof can exhaust CPU resources

Document version: 2.0

Posting date: 13 February 2024

Program impacted: BIND 9

Versions affected:

BIND

- 9.0.0 -> 9.16.46
- 9.18.0 -> 9.18.22
- 9.19.0 -> 9.19.20

(Versions prior to 9.11.37 were not assessed.)

BIND Supported Preview Edition

- 9.9.3-S1 -> 9.16.46-S1
- 9.18.11-S1 -> 9.18.22-S1

(Versions prior to 9.11.37-S1 were not assessed.)

Severity: High

Exploitable: Remotely

Description:

The processing of responses coming from DNSSEC-signed zones using NSEC3 can cause CPU exhaustion on a DNSSEC-validating resolver.

Impact:

By flooding the target resolver with queries exploiting this flaw an attacker can significantly impair the resolver's performance, effectively denying legitimate clients access to the DNS resolution service.

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:

Although this is not recommended, disabling DNSSEC validation entirely will remove the vulnerability. We instead strongly advise installing one of the versions of BIND listed below, in which an exceptionally complex DNSSEC validation will no longer impede other server workload.

We also recommend that authoritative server operators follow Best Current Practice document RFC 9276 ("Guidance for NSEC3 Parameter Settings"). Failure to adopt the RFC 9276 guidance may lead to future problems when DNS resolvers start to enforce the recommendations more strictly.

Active exploits:

This flaw was discovered in internal testing. 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, 6 February 2024
- 1.1 Revised the list of fixed versions, 11 February 2024
- 1.2 Expanded Description, Impact, and Workarounds sections, 12 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-2023-50868 is the complete and official security advisory document.

Legal Disclaimer: