

CVE-2026-1519: Excessive NSEC3 iterations cause high CPU load during insecure delegation validation

Published on Mar 25, 2026

🕒 2 minute(s) read • 🎧 Listen



CVE: [CVE-2026-1519](#)

Title: Excessive NSEC3 iterations cause high CPU load during insecure delegation validation

Document version: 2.0

Posting date: 25 March 2026

Program impacted: [BIND 9](#)

Versions affected:

BIND

- 9.11.0 -> 9.16.50
- 9.18.0 -> 9.18.46
- 9.20.0 -> 9.20.20
- 9.21.0 -> 9.21.19

BIND Supported Preview Edition

- 9.11.3-S1 -> 9.16.50-S1
- 9.18.11-S1 -> 9.18.46-S1
- 9.20.9-S1 -> 9.20.20-S1

(Versions prior to 9.11.0 were not assessed.)

Severity: High

Exploitable: Remotely

Description:

If a BIND resolver is performing DNSSEC validation and encounters a maliciously crafted zone, the resolver may consume excessive CPU. Authoritative-only servers are generally unaffected, although there are circumstances where authoritative servers may make recursive queries (see: <https://kb.isc.org/docs/why-does-my-authoritative-server-make-recursive-queries>).

Impact:

If this issue is encountered, the resolver may experience excessive CPU consumption and a sharp decrease in the number of queries per second that it can handle.

- Authoritative services are believed to be unaffected by this vulnerability but it is important to read: <https://kb.isc.org/docs/why-does-my-authoritative-server-make-recursive-queries>
- Resolvers are affected by this vulnerability.

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:

This is not recommended, but disabling DNSSEC (`dnssec-validation no;`) prevents exploitation of this issue.

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:

- 9.18.47
- 9.20.21
- 9.21.20

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

- 9.18.47-S1
- 9.20.21-S1

Acknowledgments:

ISC would like to thank Samy Medjahed/Ap4sh for bringing this vulnerability to our attention.

Document revision history:

- 1.0 Early Notification, 18 March 2026
- 2.0 Public disclosure, 25 March 2026

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](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-2026-1519> is the complete and official security advisory document.

Legal Disclaimer:

Internet Systems Consortium (ISC) is providing this notice on an "AS IS" basis. No warranty or guarantee of any kind is expressed in this notice and none should be implied. ISC expressly excludes and disclaims any warranties regarding this notice or materials referred to in this notice, including, without limitation, any implied warranty of merchantability, fitness for a particular purpose, absence of hidden defects, or of non-infringement. Your use or reliance on this notice or materials referred to in this notice is at your own risk. ISC may change this notice at any time. A stand-alone copy or paraphrase of the text of this document that omits the document URL is an uncontrolled copy. Uncontrolled copies may lack important information, be out of date, or contain factual errors.