



# Excessive NSEC3 iterations cause high CPU load during insecure delegation validation

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2026-1519
<b>State</b>	PUBLISHED
<b>Assigner</b>	isc
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2026-03-25 14:16:33 UTC
<b>Updated</b>	2026-04-13 10:16:11 UTC
<b>Description</b>	If a BIND resolver is performing DNSSEC validation and encounters a maliciously crafted zone, the resolver may consume

## Risk And Classification

**Primary CVSS:** v3.1 7.5 HIGH from security-officer@isc.org

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

**EPSS:** 0.000680000 probability, percentile 0.208600000 (date 2026-04-15)

**Problem Types:** CWE-606 | CWE-606 CWE-606 Unchecked Input for Loop Condition

Version	Source	Type	Score	Severity	Vector
3.1	security-officer@isc.org	Secondary	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
3.1	CNA	DECLARED	7.5	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

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

### Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	ISC	BIND 9	affected 9.11.0 9.16.50 custom	Not specified
CNA	ISC	BIND 9	affected 9.18.0 9.18.46 custom	Not specified
CNA	ISC	BIND 9	affected 9.20.0 9.20.20 custom	Not specified
CNA	ISC	BIND 9	affected 9.21.0 9.21.19 custom	Not specified
CNA	ISC	BIND 9	affected 9.11.3-S1 9.16.50-S1 custom	Not specified
CNA	ISC	BIND 9	affected 9.18.11-S1 9.18.46-S1 custom	Not specified
CNA	ISC	BIND 9	affected 9.20.9-S1 9.20.20-S1 custom	Not specified

### References

Reference	Source	Link	Tags
downloads.isc.org/isc/bind9/9.20.21	security-officer@isc.org	<a href="https://downloads.isc.org">downloads.isc.org</a>	
downloads.isc.org/isc/bind9/9.21.20	security-officer@isc.org	<a href="https://downloads.isc.org">downloads.isc.org</a>	
lists.debian.org/debian-lts-announce/2026/04/msg00008.html	af854a3a-2127-422b-91ae-364da2661108	<a href="https://lists.debian.org">lists.debian.org</a>	
kb.isc.org/docs/cve-2026-1519	security-officer@isc.org	<a href="https://kb.isc.org">kb.isc.org</a>	
downloads.isc.org/isc/bind9/9.18.47	security-officer@isc.org	<a href="https://downloads.isc.org">downloads.isc.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, a

### Vendor Comments And Credit

#### Discovery Credit

**CNA:** ISC would like to thank Samy Medjahed/Ap4sh for bringing this vulnerability to our attention. (en)

### Additional Advisory Data

#### Solutions

**CNA:** Upgrade to the patched release most closely related to your current version of BIND 9: 9.18.47, 9.20.21, 9.21.20, 9.18.47-S1, or 9.20.21-S1.

## Workarounds

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

## Exploits

**CNA:** We are not aware of any active exploits.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)