



# CVE-2023-26249

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2023-26249
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-02-21 02:15:00 UTC
<b>Updated</b>	2023-03-02 23:20:00 UTC
<b>Description</b>	Knot Resolver before 5.6.0 enables attackers to consume its resources, launching amplification attacks and potentially causing denial of service.

## Risk And Classification

**Problem Types:** CWE-770

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nic	Knot Resolver	All	All	All	All

## References

Reference	Source	Link	Tags
Knot Resolver 5.6.0 released – Knot Resolver	MISC	<a href="http://www.knot-resolver.cz">www.knot-resolver.cz</a>	
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

182024 Debian Security Update for knot-resolver (CVE-2023-26249)

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](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)