



# CVE-2018-10920

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2018-10920
<b>State</b>	PUBLIC
<b>Assigner</b>	secalert@redhat.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2018-08-02 13:29:00 UTC
<b>Updated</b>	2020-02-18 19:06:00 UTC
<b>Description</b>	Improper input validation bug in DNS resolver component of Knot Resolver before 2.4.1 allows remote attacker to poison ca

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nic	<a href="#">Knot Resolver</a>	All	All	All	All
Application	Nic	<a href="#">Knot Resolver</a>	All	All	All	All

## References

Reference	Source	Link
1610951 – (CVE-2018-10920) CVE-2018-10920 knot-resolver: Improper input validation bug in DNS resolver component	CONFIRM	<a href="#">bugz</a>
Knot Resolver 2.4.1 released – Knot Resolver	CONFIRM	<a href="#">www</a>
CVE Program record	CVE.ORG	<a href="#">www</a>
NVD vulnerability detail	NVD	<a href="#">nvd.r</a>

No vendor comments have been submitted for this CVE.

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

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](#).

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