



CVE-2019-10190

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

Summary

CVE	CVE-2019-10190
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-16 18:15:00 UTC
Updated	2023-02-12 23:33:00 UTC
Description	A vulnerability was discovered in DNS resolver component of knot resolver through version 3.2.0 before 4.1.0 which allows

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	30	All	All	All
Application	Nic	Knot Resolver	All	All	All	All
Application	Nic	Knot Resolver	All	All	All	All
Application	Nic	Knot Resolver	All	All	All	All

References

Reference

[SECURITY] Fedora 30 Update: knot-resolver-4.1.0-1.fc30 - package-announce - Fedora Mailing-Lists
Knot Resolver 4.1.0 released – Knot Resolver
[SECURITY] Fedora 30 Update: knot-resolver-4.1.0-1.fc30 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 29 Update: knot-resolver-4.1.0-1.fc29 - package-announce - Fedora Mailing-Lists
1727208 – (CVE-2019-10190) CVE-2019-10190 knot-resolver: improper input validation in DNS resolver allows remote attacker to bypass DN
[SECURITY] Fedora 29 Update: knot-resolver-4.1.0-1.fc29 - package-announce - Fedora Mailing-Lists
CVE Program record

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501027 Alpine Linux Security Update for knot-resolver

© [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](#).

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