



CVE-2019-3807

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

Summary

| | |
|------------------------|--|
| CVE | CVE-2019-3807 |
| State | PUBLIC |
| Assigner | secalert@redhat.com |
| Source Priority | CVE Program / NVD first with legacy fallback |
| Published | 2019-01-29 17:29:00 UTC |
| Updated | 2019-10-09 23:49:00 UTC |
| Description | An issue has been found in PowerDNS Recursor versions 4.1.x before 4.1.9 where records in the answer section of respon |

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|-------------|----------|----------|---------|--------|---------|----------|
| Application | Powerdns | Recursor | All | All | All | All |

References

| Reference | Source | L |
|--|---------|----|
| 1669151 – (CVE-2019-3807) CVE-2019-3807 pdns-recursor: Insufficient validation of DNSSEC signature | CONFIRM | bl |
| PowerDNS Security Advisory 2019-02: Insufficient validation of DNSSEC signatures — PowerDNS Recursor documentation | CONFIRM | dl |
| CVE Program record | CVE.ORG | w |
| NVD vulnerability detail | NVD | n |

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[501114](#) Alpine Linux Security Update for pdns-recursor

[505209](#) Alpine Linux Security Update for pdns-recursor

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](#)