



CVE-2018-10851

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2018-10851
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-11-29 18:29:00 UTC
Updated	2019-10-09 23:33:00 UTC
Description	PowerDNS Authoritative Server 3.3.0 up to 4.1.4 excluding 4.1.5 and 4.0.6, and PowerDNS Recursor 3.2 up to 4.1.4 excluding 4.1.5 and 4.0.6

Risk And Classification

Problem Types: CWE-772

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Powerdns	Authoritative	All	All	All	All
Application	Powerdns	Recursor	All	All	All	All

References

Reference

- PowerDNS Security Advisory 2018-03: Crafted zone record can cause a denial of service — PowerDNS Authoritative Server documentation
- PowerDNS Security Advisory 2018-04: Crafted answer can cause a denial of service — PowerDNS Recursor documentation
- 1588185 – (CVE-2018-10851) CVE-2018-10851 pdns: Memory leak while parsing malformed records
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501112 Alpine Linux Security Update for pdns-recursor

501121 Alpine Linux Security Update for pdns

501122 Alpine Linux Security Update for pdns-recursor

© [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](#)