



CVE-2019-3806

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

Summary

CVE	CVE-2019-3806
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-01-29 17:29:00 UTC
Updated	2020-10-19 17:45:00 UTC
Description	An issue has been found in PowerDNS Recursor versions after 4.1.3 before 4.1.9 where Lua hooks are not properly applied

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source
PowerDNS Security Advisory 2019-01: Lua hooks are not applied in certain configurations — PowerDNS Recursor documentation	CONFIRMED
1669421 – (CVE-2019-3806) CVE-2019-3806 pdns-recursor: Lua hooks are not applied in certain configuration	CONFIRMED
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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

© [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](#)