



CVE-2019-3871

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

Summary

CVE	CVE-2019-3871
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 21:29:00 UTC
Updated	2023-11-07 03:10:00 UTC
Description	A vulnerability was found in PowerDNS Authoritative Server before 4.0.7 and before 4.1.7. An insufficient validation of data

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	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Operating System	Fedoraproject	Fedora	28	All	All	All
Operating System	Fedoraproject	Fedora	29	All	All	All
Application	Powerdns	Authoritative Server	All	All	All	All
Application	Powerdns	Authoritative Server	All	All	All	All

References

Reference

Debian -- Security Information -- DSA-4424-1 pdns
[SECURITY] [DLA 1737-1] pdns security update
Bugtraq: [SECURITY] [DSA 4424-1] pdns security update
PowerDNS Security Advisory 2019-03: Insufficient validation in the HTTP remote backend — PowerDNS Authoritative Server documentation
oss-security - PowerDNS Security Advisory 2019-03
[SECURITY] Fedora 28 Update: pdns-4.1.7-1.fc28 - package-announce - Fedora Mailing-Lists
1689013 – (CVE-2019-3871) CVE-2019-3871 pdns: insufficient validation of data when building a HTTP request from a DNS query
[SECURITY] Fedora 28 Update: pdns-4.1.7-1.fc28 - package-announce - Fedora Mailing-Lists

[SECURITY] Fedora 29 Update: pdns-4.1.7-1.fc29 - package-announce - Fedora Mailing-Lists

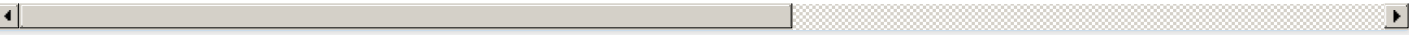
[security-announce] openSUSE-SU-2019:1128-1: important: Security update

PowerDNS Authoritative Server CVE-2019-3871 Denial of Service Vulnerability

[SECURITY] Fedora 29 Update: pdns-4.1.7-1.fc29 - package-announce - Fedora Mailing-Lists

CVE Program record

NVD vulnerability detail



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[375500](#) PowerDNS Authoritative Server Information Disclosure Vulnerability

[501122](#) Alpine Linux Security Update for pdns

© [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](#)