



CVE-2020-17482

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

Summary

CVE	CVE-2020-17482
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-10-02 09:15:00 UTC
Updated	2022-01-01 18:15:00 UTC
Description	An issue has been found in PowerDNS Authoritative Server before 4.3.1 where an authorized user with the ability to insert c

Risk And Classification

Problem Types: CWE-908

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference
PowerDNS/pdns · GitHub
PowerDNS Security Advisory 2020-05: Leaking uninitialised memory through crafted zone records — PowerDNS Authoritative Server documenta
PowerDNS: information disclosure (GLSA 202012-18) — Gentoo security
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501123 Alpine Linux Security Update for pdns
501657 Alpine Linux Security Update for pdns
20201115 Debian Security Advisory (DSA) 4589-1 for pdns

[690544](#) Free Berkeley Software Distribution (FreeBSD) Security Update for powerdns (b3/1db92-1e34-11ea-b90e-6805ca21a2/1)

[750621](#) OpenSUSE Security Update for pdns (openSUSE-SU-2020:1556-1)

© [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](#)