



CVE-2020-10995

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

Summary

CVE	CVE-2020-10995
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-05-19 17:15:00 UTC
Updated	2023-11-07 03:14:00 UTC
Description	PowerDNS Recursor from 4.1.0 up to and including 4.3.0 does not sufficiently defend against amplification attacks. An issue

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Opensuse	Backports Sle	15.0	sp1	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Application	Powerdns	Recursor	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 31 Update: pdns-recursor-4.2.2-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
PowerDNS Security Advisory 2020-01: Denial of Service — PowerDNS Recursor documentation	CONFIRM	doc.powerdns.com
NXNSAttack	MISC	www.nxnsattack.com
[security-announce] openSUSE-SU-2020:0698-1: moderate: Security update f	SUSE	lists.opensuse.org
[SECURITY] Fedora 32 Update: pdns-recursor-4.3.1-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
Debian -- Security Information -- DSA-4691-1 pdns-recursor	DEBIAN	www.debian.org
[SECURITY] Fedora 32 Update: pdns-recursor-4.3.1-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.org
[SECURITY] Fedora 31 Update: pdns-recursor-4.2.2-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
No vendor comments have been submitted for this CVE.		
Legacy QID Mappings		
501115 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