



CVE-2018-1000003

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

Summary

CVE	CVE-2018-1000003
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-01-22 18:29:00 UTC
Updated	2018-02-06 14:06:00 UTC
Description	Improper input validation bugs in DNSSEC validators components in PowerDNS version 4.1.0 allow attacker in man-in-the-

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Powerdns	Recursor	4.1.0	All	All	All
Application	Powerdns	Recursor	4.1.0	All	All	All

References

Reference	Source	L
PowerDNS Security Advisory 2018-01: Insufficient validation of DNSSEC signatures — PowerDNS Recursor documentation	CONFIRM	d
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

501111 Alpine Linux Security Update for pdns-recursor

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](#)