



CVE-2016-6172

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

Summary

CVE	CVE-2016-6172
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-09-26 16:59:00 UTC
Updated	2018-10-30 16:27:00 UTC
Description	PowerDNS (aka pdns) Authoritative Server before 4.0.1 allows remote primary DNS servers to cause a denial of service (m

Risk And Classification


Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Application	Powerdns	Authoritative Server	All	All	All	All

References

Reference	Source
Add limits to the size of received {A,I}XFR, in megabytes by rgacogne · Pull Request #4133 · PowerDNS/pdns · GitHub	CO
openSUSE-SU-2016:2116-1: moderate: Security update for pdns	SI
PowerDNS AXFR/IXFR Response Processing Bug Lets Remote DNS Servers Cause the Target DNS Service to Crash - SecurityTracker	SI
Debian -- Security Information -- DSA-3664-1 pdns	DI
xfer size issue · Issue #4128 · PowerDNS/pdns · GitHub	CO
Add limits to the size of received AXFR, in megabytes by rgacogne · Pull Request #4134 · PowerDNS/pdns · GitHub	CO
[dns-operations] DNS activities in Japan	M
Multiple DNS Servers Remote Denial of Service Vulnerability	BI
oss-security - Malicious primary DNS servers can crash secondaries	M

Changelogs	CO
xfer-limit/README.md at master · sischkg/xfer-limit · GitHub	M
CVE Program record	C'
NVD vulnerability detail	N'
	
<p>No vendor comments have been submitted for this CVE.</p>	
<p>There are currently no legacy QID mappings associated with this CVE.</p>	

© [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](#)