



CVE-2016-7072

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

Summary

CVE	CVE-2016-7072
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-10 17:29:00 UTC
Updated	2019-10-09 23:19:00 UTC
Description	An issue has been found in PowerDNS Authoritative Server before 3.4.11 and 4.0.2 allowing a remote, unauthenticated attacker to perform a denial of service attack.

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	8.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Powerdns	Authoritative	All	All	All	All
Application	Powerdns	Authoritative	All	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-3764-1 pdns	DEBIAN	www.debian.org	Third Party Advisory
1627328 -- (CVE-2016-7072) CVE-2016-7072 pdns: Denial of service via the web server	CONFIRM	bugzilla.redhat.com	Issue Tracking, Vulnerability
Advisory 2016-03	CONFIRM	doc.powerdns.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)