



CVE-2015-1868

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

Summary

CVE	CVE-2015-1868
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-05-18 15:59:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The label decompression functionality in PowerDNS Recursor 3.5.x, 3.6.x before 3.6.3, and 3.7.x before 3.7.2 and Authorita

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

AV:N/AC:L/Au:N/C:N/I:N/A:C

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:N/AC:L/Au:N/C:N/I:N/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	20	All	All	All

Operating System	Fedora project	Fedora	21	All	All	All
Operating System	Fedora project	Fedora	22	All	All	All
Application	Powerdns	Authoritative	3.2	All	All	All
Application	Powerdns	Authoritative	3.3	All	All	All
Application	Powerdns	Authoritative	3.3.1	All	All	All
Application	Powerdns	Authoritative	3.3.2	All	All	All
Application	Powerdns	Authoritative	3.4.0	All	All	All
Application	Powerdns	Authoritative	3.4.1	All	All	All
Application	Powerdns	Authoritative	3.4.3	All	All	All
Application	Powerdns	Recursor	3.5	All	All	All
Application	Powerdns	Recursor	3.5.1	All	All	All
Application	Powerdns	Recursor	3.5.2	All	All	All
Application	Powerdns	Recursor	3.5.3	All	All	All
Application	Powerdns	Recursor	3.6.0	All	All	All
Application	Powerdns	Recursor	3.6.1	All	All	All
Application	Powerdns	Recursor	3.6.2	All	All	All
Application	Powerdns	Recursor	3.6.3	All	All	All
Application	Powerdns	Recursor	3.7.1	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference				Source	Link	
Debian -- Security Information -- DSA-3306-1 pdns				af854a3a-2127-422b-91ae-364da2661108	www	
[SECURITY] Fedora 22 Update: pdns-3.4.4-1.fc22				af854a3a-2127-422b-91ae-364da2661108	lists	
[SECURITY] Fedora 20 Update: pdns-3.3.1-3.fc20				af854a3a-2127-422b-91ae-364da2661108	lists	
[SECURITY] Fedora 20 Update: pdns-recursor-3.7.2-1.fc20				af854a3a-2127-422b-91ae-364da2661108	lists	
Multiple PowerDNS Products CVE-2015-1868 Remote Denial of Service Vulnerability				af854a3a-2127-422b-91ae-364da2661108	www	
Debian -- Security Information -- DSA-3307-1 pdns-recursor				af854a3a-2127-422b-91ae-364da2661108	www	
[SECURITY] Fedora 22 Update: pdns-recursor-3.7.2-1.fc22				af854a3a-2127-422b-91ae-364da2661108	lists	
PowerDNS Label Decompression Bug Lets Remote Users Deny Service - SecurityTracker				af854a3a-2127-422b-91ae-364da2661108	www	
[SECURITY] Fedora 21 Update: pdns-3.4.4-1.fc21				af854a3a-2127-422b-91ae-364da2661108	lists	
[SECURITY] Fedora 21 Update: pdns-recursor-3.7.2-1.fc21				af854a3a-2127-422b-91ae-364da2661108	lists	
CVE Program record				CVE.ORG	www	
NVD vulnerability detail				NVD	nvd	

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](#)