



CVE-2009-4009

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

Summary

CVE	CVE-2009-4009
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-01-08 17:30:00 UTC
Updated	2018-10-10 19:48:00 UTC
Description	Buffer overflow in PowerDNS Recursor before 3.1.7.2 allows remote attackers to cause a denial of service (daemon crash)

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Powerdns	Recursor	2.0_rc1	All	All	All
Application	Powerdns	Recursor	2.8	All	All	All
Application	Powerdns	Recursor	2.9.15	All	All	All
Application	Powerdns	Recursor	2.9.16	All	All	All
Application	Powerdns	Recursor	2.9.17	All	All	All
Application	Powerdns	Recursor	2.9.18	All	All	All
Application	Powerdns	Recursor	3.0	All	All	All
Application	Powerdns	Recursor	3.0.1	All	All	All
Application	Powerdns	Recursor	3.1	All	All	All
Application	Powerdns	Recursor	3.1.1	All	All	All
Application	Powerdns	Recursor	3.1.2	All	All	All
Application	Powerdns	Recursor	3.1.3	All	All	All
Application	Powerdns	Recursor	3.1.4	All	All	All
Application	Powerdns	Recursor	3.1.5	All	All	All
Application	Powerdns	Recursor	3.1.6	All	All	All
Application	Powerdns	Recursor	3.1.7	All	All	All
Application	Powerdns	Recursor	3.1.7.1	All	All	All

Application	Powerdns	Recursor	2.0_rc1	All	All	All
Application	Powerdns	Recursor	2.8	All	All	All
Application	Powerdns	Recursor	2.9.15	All	All	All
Application	Powerdns	Recursor	2.9.16	All	All	All
Application	Powerdns	Recursor	2.9.17	All	All	All
Application	Powerdns	Recursor	2.9.18	All	All	All
Application	Powerdns	Recursor	3.0	All	All	All
Application	Powerdns	Recursor	3.0.1	All	All	All
Application	Powerdns	Recursor	3.1	All	All	All
Application	Powerdns	Recursor	3.1.1	All	All	All
Application	Powerdns	Recursor	3.1.2	All	All	All
Application	Powerdns	Recursor	3.1.3	All	All	All
Application	Powerdns	Recursor	3.1.4	All	All	All
Application	Powerdns	Recursor	3.1.5	All	All	All
Application	Powerdns	Recursor	3.1.6	All	All	All
Application	Powerdns	Recursor	3.1.7	All	All	All
Application	Powerdns	Recursor	3.1.7.1	All	All	All
Application	Powerdns	Recursor	All	All	All	All

References						
Reference				Source		
Fedora update for pdns-recursor - Secunia Advisories - Vulnerability Information - Secunia.com				SECUNIA		
Bug 552285 – CVE-2009-4009 CVE-2009-4010 PowerDNS Recursor: code execution and domain spoofing flaws				CONFIRMED		
[SECURITY] Fedora 12 Update: pdns-recursor-3.1.7.2-1.fc12				FEDORA		
IBM X-Force Exchange				XF		
SecurityFocus				BUGTRAQ		
PowerDNS Recursor Spoofing and Buffer Overflow Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com				SECUNIA		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VULNERABILITIES		
PowerDNS Recursor Buffer Overflow May Let Remote Users Execute Arbitrary Code - SecurityTracker				SECURITYTRACKER		
PowerDNS Recursor Buffer Overflow Vulnerability				BID		
[SECURITY] Fedora 11 Update: pdns-recursor-3.1.7.2-1.fc11				FEDORA		
PowerDNS Security Advisory 2010-01: PowerDNS Recursor up to and including 3.1.7.1 can be brought down and probably exploited				CONFIRMED		
CVE Program record				CVE.COM		
NVD vulnerability detail				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](#)