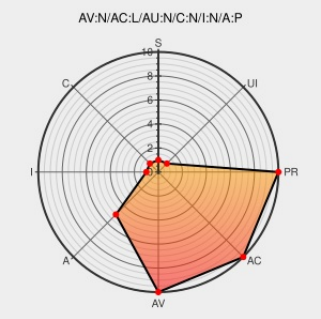
CVE-2015-5311

Published on: 11/17/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

CVE-2015-5311

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Authoritative from Powerdns contain the following vulnerability:

PowerDNS (aka pdns) Authoritative Server 3.4.4 before 3.4.7 allows remote attackers to cause a denial of service (assertion failure and server crash) via crafted query packets.

CVE-2015-5311 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Advisory 2015-03	Patch, Vendor Advisory, doc.powerdns.com, text/html	CONFIRM doc.powerdns.com/md/security/powerdns-advisory-2015-03/
PowerDNS Authoritative Server Packet Processing Flaw Lets Remote Users Cause the Target Service to Crash - SecurityTracker	www.securitytracker.com, text/html	SECTRACK 1034098
[SECURITY] Fedora 22 Update: pdns-3.4.7-1.fc22	lists.fedoraproject.org, text/html	FEDORA FEDORA-2015-1d49176aa1
oss-security - PowerDNS Security Announcement 2015-03	www.openwall.com, text/html	MLIST [oss-security] 20151109 PowerDNS Security Announcement 2015-03
[SECURITY] Fedora 23 Update: pdns-3.4.7-1.fc23	lists.fedoraproject.org, text/html	FEDORA FEDORA-2015-8b8d94ebbb

[SECURITY] Fedora 21 Update: pdns-3.4.7-1.fc21	lists.fedoraproject.org text/html	FEDORA FEDORA-2015-a3965fd800

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Powerdns	Authoritative	3.4.4	All	All	All
Application	Powerdns	Authoritative	3.4.5	All	All	All
Application	Powerdns	Authoritative	3.4.6	All	All	All
Application	Powerdns	Authoritative	3.4.4	All	All	All
Application	Powerdns	Authoritative	3.4.5	All	All	All
Application	Powerdns	Authoritative	3.4.6	All	All	All

cpe:2.3:a:powerdns:authoritative:3.4.4:*:*:*:*:*:*:*

cpe:2.3:a:powerdns:authoritative:3.4.5:*:*:*:*:*:*:*

cpe:2.3:a:powerdns:authoritative:3.4.6:*:*:*:*:*:*:*

cpe:2.3:a:powerdns:authoritative:3.4.4:*:*:*:*:*:*:*

cpe:2.3:a:powerdns:authoritative:3.4.5:*:*:*:*:*:*:*

cpe:2.3:a:powerdns:authoritative:3.4.6:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→