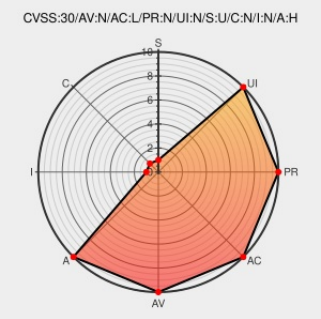
CVE-2016-5426

Published on: 09/21/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-5426

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



Certain versions of Authoritative from Powerdns contain the following vulnerability:

PowerDNS (aka pdns) Authoritative Server before 3.4.10 allows remote attackers to cause a denial of service (backend CPU consumption) via a long qname.

CVE-2016-5426 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	NONE	NONE	HIGH

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 2016-01	Vendor Advisory, doc.powerdns.com, text/html	CONFIRM doc.powerdns.com/md/security/powerdns-advisory-2016-01/
Debian -- Security	www.debian.org	DEBIAN DSA-3664

Information -- DSA-3664-1 pdns	Depreciated Link text/html	
oss-security - PowerDNS Security Advisory 2016-01: Crafted queries can cause unexpected backend load	Release Notes www.openwall.com text/html	MLIST [oss-security] 20160909 PowerDNS Security Advisory 2016-01: Crafted queries can cause unexpected backend load
PowerDNS Authoritative Server Query Processing Flaws Let Remote Users Consume Excessive Resources on the Target Backend System - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1036761
Reject qname's wirelength > 255, `chopOff()` handle dot inside labels · PowerDNS/pdns@881b5b0 · GitHub	Patch github.com text/html	CONFIRM github.com/PowerDNS/pdns/commit/881b5b03a590198d03008e4200dd00cc537712f
PowerDNS Multiple Denial of Service Vulnerabilities	cve.report (archive) text/html	BID 92917

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	All	All	All	All

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

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→