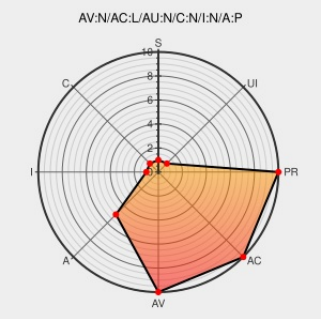
CVE-2006-2076

Published on: 04/27/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:08 PM UTC

CVE-2006-2076

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



Certain versions of Pdnsd from Pdnsd contain the following vulnerability:

Memory leak in Paul Rombouts pdnsd before 1.2.4 allows remote attackers to cause a denial of service (memory consumption) via a DNS query with an unsupported (1) QTYPE or (2) QCLASS, as demonstrated by the OUSPG PROTOS DNS test suite.

CVE-2006-2076 has been assigned by cve@mitre.org 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
pdnsd DNS Query Handling Memory Leak Vulnerability - Advisories - Secunia	web.archive.org, text/html	SECUNIA 19835
Secunia - Advisories - Gentoo update for pdnsd	web.archive.org, text/html	SECUNIA 20055
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF dns-improper-request-handling(26081)
	Vendor Advisory, www.niscc.gov.uk, application/pdf, Inactive Link, Not Archived	MISC www.niscc.gov.uk/niscc/docs/re-20060425-00312.pdf?lang=en
No Description Provided	Vendor Advisory, web.archive.org, text/html	MISC www.niscc.gov.uk/niscc/docs/br-20060425-00311.html?lang=en

	Inactive Link Not Archived	
pdnsd Bug in Processing ADNS Queries Lets Remote Users Deny Service - SecurityTracker	Patch securitytracker.com text/html	SECTRACK 1015989
Paul A. Rombouts PDNSD DNS Query Denial Of Service Vulnerability	Patch cve.report (archive) text/html	BID 17694
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2006-1505
US-CERT Vulnerability Note VU#955777	US Government Resource www.kb.cert.org text/html	CERT-VN VU#955777
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	VUPEN ADV-2006-1528
pdnsd maintenance page by Paul Rombouts	www.phys.uu.nl text/html	CONFIRM www.phys.uu.nl/~rombouts/pdnsd.html
Gentoo Linux Documentation -- pdnsd: Denial of Service and potential arbitrary code execution	www.gentoo.org text/html	GENTOO GLSA-200605-10

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pdnsd	Pdnsd	1.0.13	All	All	All
Application	Pdnsd	Pdnsd	1.0.15	All	All	All
Application	Pdnsd	Pdnsd	1.1	All	All	All
Application	Pdnsd	Pdnsd	1.1.1	All	All	All
Application	Pdnsd	Pdnsd	1.1.10_par	All	All	All
Application	Pdnsd	Pdnsd	1.1.11_par	All	All	All
Application	Pdnsd	Pdnsd	1.1.2	All	All	All
Application	Pdnsd	Pdnsd	1.1.3	All	All	All
Application	Pdnsd	Pdnsd	1.1.4	All	All	All
Application	Pdnsd	Pdnsd	1.1.5	All	All	All
Application	Pdnsd	Pdnsd	1.1.6	All	All	All
Application	Pdnsd	Pdnsd	1.1.7a	All	All	All
Application	Pdnsd	Pdnsd	1.1.8b1_par5	All	All	All
Application	Pdnsd	Pdnsd	1.1.8b1_par6	All	All	All

Application	Pdnsd	Pdnsd	1.1.8b1_par8	All	All	All
Application	Pdnsd	Pdnsd	1.2.1_par	All	All	All
Application	Pdnsd	Pdnsd	1.2.2_par	All	All	All
Application	Pdnsd	Pdnsd	1.2.3_par	All	All	All
Application	Pdnsd	Pdnsd	1.0.13	All	All	All
Application	Pdnsd	Pdnsd	1.0.15	All	All	All
Application	Pdnsd	Pdnsd	1.1	All	All	All
Application	Pdnsd	Pdnsd	1.1.1	All	All	All
Application	Pdnsd	Pdnsd	1.1.10_par	All	All	All
Application	Pdnsd	Pdnsd	1.1.11_par	All	All	All
Application	Pdnsd	Pdnsd	1.1.2	All	All	All
Application	Pdnsd	Pdnsd	1.1.3	All	All	All
Application	Pdnsd	Pdnsd	1.1.4	All	All	All
Application	Pdnsd	Pdnsd	1.1.5	All	All	All
Application	Pdnsd	Pdnsd	1.1.6	All	All	All
Application	Pdnsd	Pdnsd	1.1.7a	All	All	All
Application	Pdnsd	Pdnsd	1.1.8b1_par5	All	All	All
Application	Pdnsd	Pdnsd	1.1.8b1_par6	All	All	All
Application	Pdnsd	Pdnsd	1.1.8b1_par8	All	All	All
Application	Pdnsd	Pdnsd	1.2.1_par	All	All	All
Application	Pdnsd	Pdnsd	1.2.2_par	All	All	All
Application	Pdnsd	Pdnsd	1.2.3_par	All	All	All

cpe:2.3:a:pdnsd:pdnsd:1.0.13:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.0.15:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.10_par:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.11_par:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.7a:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.8b1_par5:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.8b1_par6:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.8b1_par8:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.2.1_par:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.2.2_par:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.2.3_par:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.0.13:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.0.15:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.10_par:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.11_par:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.4:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.5:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.6:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.7a:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.8b1_par5:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.8b1_par6:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.1.8b1_par8:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.2.1_par:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.2.2_par:*:*:*:*:*:*:*:

cpe:2.3:a:pdnsd:pdnsd:1.2.3_par:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report