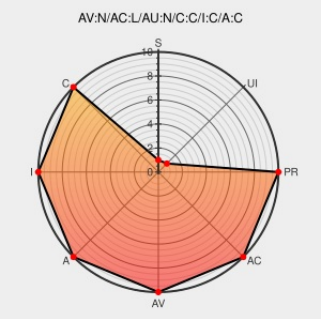
CVE-2006-2077

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

Last Modified on: 03/23/2021 11:25:07 PM UTC

CVE-2006-2077

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



Certain versions of Pdnsd from Pdnsd contain the following vulnerability:

Buffer overflow in Paul Rombouts pdnsd before 1.2.4 has unknown impact and attack vectors. NOTE: this issue might be related to the OUSPG PROTOS DNS test suite.

CVE-2006-2077 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link
Secunia - Advisories - Gentoo update for pdnsd	web.archive.org text/html	SECUNIA 20055
Paul A. Rombouts PDNSD Unspecified Buffer Overflow Vulnerability	cve.report (archive) text/html	BID 17720
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF dns-improper-request-handling(26081)
US-CERT Vulnerability Note VU#955777	US Government Resource www.kb.cert.org text/html	CERT-VN VU#955777
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	www.gentoo.org	GENTOO GLSA-200605-10

potential arbitrary code execution text/html

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	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→