CVE-2009-0858

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2009-0858
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-03-09 21:30:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The response_addname function in response.c in Daniel J. Bernstein djbdns 1.05 and earlier does not constrain offsets in t

Risk And Classification

Primary CVSS: v2.0 5.8 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:P

Problem Types: CWE-20 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:N/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	D.j.bernstein	Djbdns	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source	Link
Debian -- Security Information -- DSA-1831-1 djbdns	af854a3a-2127-422b-91ae-364da2661108	www.
'djbdns misformats some long response packets; patch and example' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.
Debian update for djbdns - Secunia Advisories - Vulnerability Information - Secunia.com	af854a3a-2127-422b-91ae-364da2661108	secun
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.
Dan Bernstein Confirms Security Flaw In Djbdns - Slashdot	af854a3a-2127-422b-91ae-364da2661108	it.slas
Security issue in djbdns confirmed | Security and the Net	af854a3a-2127-422b-91ae-364da2661108	secur
IBM X-Force Exchange	af854a3a-2127-422b-91ae-364da2661108	excha
'djbdns<=1.05 lets AXFRed subdomains overwrite domains' - MARC	af854a3a-2127-422b-91ae-364da2661108	marc.
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.
djbdns Long Response Packet Remote Cache Poisoning Vulnerability	af854a3a-2127-422b-91ae-364da2661108	www.
SecurityFocus	af854a3a-2127-422b-91ae-364da2661108	www.
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.