



CVE-2008-4392

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2008-4392
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-02-19 16:30:00 UTC
Updated	2017-08-08 01:32:00 UTC
Description	dnscache in Daniel J. Bernstein djbdns 1.05 does not prevent simultaneous identical outbound DNS queries, which makes

Risk And Classification

Problem Types: CWE-362

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	D.j.bernstein	Djbdns	1.05	All	All	All
Application	D.j.bernstein	Djbdns	1.05	All	All	All

References

Reference	Source	Lir
djbdns SOA Requests DNS Cache Poisoning Security Issue - Secunia Advisories - Vulnerability Information - Secunia.com	SECUNIA	sec
IBM X-Force Exchange	XF	exc
djbdns dnscache SOA Requests Remote Cache Poisoning Vulnerability	BID	ww
www.your.org/dnscache/djbdns.pdf	MISC	ww
djbdns patches	MISC	ww
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)