



CVE-2009-1255

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

Summary

CVE	CVE-2009-1255
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-04-30 20:30:00 UTC
Updated	2018-10-10 19:35:00 UTC
Description	The process_stat function in (1) Memcached before 1.2.8 and (2) MemcachedDB 1.2.0 discloses (a) the contents of /proc/se

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Memcachedb	Memcached	0.0.1	All	All	All
Application	Memcachedb	Memcached	0.0.2	All	All	All
Application	Memcachedb	Memcached	0.0.3	All	All	All
Application	Memcachedb	Memcached	0.0.4	All	All	All
Application	Memcachedb	Memcached	0.1.0	All	All	All
Application	Memcachedb	Memcached	0.1.1	All	All	All
Application	Memcachedb	Memcached	1.0.0	beta	All	All
Application	Memcachedb	Memcached	1.0.1	beta	All	All
Application	Memcachedb	Memcached	1.0.2	beta	All	All
Application	Memcachedb	Memcached	1.0.3	All	All	All
Application	Memcachedb	Memcached	1.0.4	All	All	All
Application	Memcachedb	Memcached	1.1.0	beta	All	All
Application	Memcachedb	Memcached	1.2.0	beta	All	All
Application	Memcachedb	Memcached	1.2.1	beta	All	All
Application	Memcachedb	Memcached	0.0.1	All	All	All
Application	Memcachedb	Memcached	0.0.2	All	All	All
Application	Memcachedb	Memcached	0.0.3	All	All	All

Application	Memcachedb	Memcached	0.0.4	All	All	All
Application	Memcachedb	Memcached	0.1.0	All	All	All
Application	Memcachedb	Memcached	0.1.1	All	All	All
Application	Memcachedb	Memcached	1.0.0	beta	All	All
Application	Memcachedb	Memcached	1.0.1	beta	All	All
Application	Memcachedb	Memcached	1.0.2	beta	All	All
Application	Memcachedb	Memcached	1.0.3	All	All	All
Application	Memcachedb	Memcached	1.0.4	All	All	All
Application	Memcachedb	Memcached	1.1.0	beta	All	All
Application	Memcachedb	Memcached	1.2.0	beta	All	All
Application	Memcachedb	Memcached	1.2.1	beta	All	All
Application	Memcachedb	Memcached	All	All	All	All

References						
Reference				Source		
20090428 Positron Security Advisory #2009-001: Memcached and MemcacheDB ASLR Bypass Weakness				FULLDISC		
memcached Discloses Application Memory Contents and Information to Remote Users - SecurityTracker				SECTRAK		
SecurityFocus				BUGTRAQ		
MemcacheDB "stats maps" Information Disclosure Weakness - Secunia Advisories - Vulnerability Information - Secunia.com				SECUNIA		
Support / Security / Advisories // MDVSA-2009:105 Mandriva				MANDRIVA		
Memcached and MemcacheDB ASLR Information Disclosure Weakness				BID		
54127				OSVDB		
Fedora update for memcached - Advisories - Community				SECUNIA		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN		
r98 - memcachedb - A distributed key-value storage system designed for persistent. - Google Project Hosting				CONFIRM		
[SECURITY] Fedora 11 Update: memcached-1.2.8-1.fc11				FEDORA		
Positron Security LLC: Security Advisory #2009-001: Memcached and MemcacheDB ASLR Bypass Weakness				MISC		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				VUPEN		
Google Groups				CONFIRM		
memcached ""stats maps" Information Disclosure Weakness - Secunia Advisories - Vulnerability Information - Secunia.com				SECUNIA		
Google Code Archive - Long-term storage for Google Code Project Hosting.				CONFIRM		
[SECURITY] Fedora 10 Update: memcached-1.2.8-1.fc10				FEDORA		
IBM X-Force Exchange				XF		
ChangeLog - memcachedb - Project Hosting on Google Code				CONFIRM		
CVE Program record				CVE.ORG		
NVD - CVE-2009-0428				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](#)