



CVE-2007-6418

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

Summary

CVE	CVE-2007-6418
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-12-18 00:46:00 UTC
Updated	2008-11-15 07:04:00 UTC
Description	The libdspam7-drv-mysql cron job in Debian GNU/Linux includes the MySQL dspam database password in a command line

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	All	All	All	All
Operating System	Debian	Debian Linux	All	All	All	All

References

Reference	Source
44138	OSVDB
Security Advisory SA29059 - Debian update for dspam - Secunia	SECUNIA
Debian -- Security Information -- DSA-1501-1 dspam	DEBIAN
#448519 - libdspam7-drv-mysql: CVE-2007-6418 cron job may disclose dspam database password to users - Debian Bug report logs	CONFIDENTIAL
DSPAM Debian 'libdspam7-drv-mysql' Cron Job MySQL Calls Local Information Disclosure Vulnerability	BID
CVE Program record	CVE.COM
NVD vulnerability detail	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](#)