



CVE-2009-0125

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

Summary

CVE	CVE-2009-0125
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-15 17:30:00 UTC
Updated	2023-11-07 02:03:00 UTC
Description	** DISPUTED ** NOTE: this issue has been disputed by the upstream vendor. nasl/nasl_crypto2.c in the Nessus Attack Scr

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Finkproject	Libnasl	2.2.11	All	All	All
Application	Finkproject	Libnasl	2.2.11	All	All	All

References

Reference	Source	Link
oss-security - CVE Request -- tsqllib, slurm-llnl, libnasl, libcrypt-openssl-dsa-perl, erlang, boinc-client, m2crypto	MLIST	openwall.com
[VIM] CVE-2009-0125 (fwd)	VIM	www.attrition.c
Bug 479655 – CVE-2009-0125 libnasl: OpenSSL incorrect checks for malformed signatures	CONFIRM	bugzilla.redhat
#511517 - libnasl: Return values of DSA_do_verify - Debian Bug report logs	MISC	bugs.debian.o
cvs.fedoraproject.org/viewvc/rpms/libnasl/F-10/libnasl.spec	CONFIRM	cvs.fedoraproj
[security-announce] SUSE Security Summary Report: SUSE-SR:2009:003	SUSE	lists.opensuse
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)