



CVE-2009-0127

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

Summary

CVE	CVE-2009-0127
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 ** M2Crypto does not properly check the return value from the OpenSSL EVP_VerifyFinal, DSA_verify, ECD

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Heikkitoivonen	M2crypto	-	All	All	All
Application	Heikki Toivonen	M2crypto	-	All	All	All
Application	Heikki Toivonen	M2crypto	-	All	All	All

References

Reference	Source	Link
oss-security - CVE Request -- tsqllib, slurm-lnl, libnasl, libcrypt-openssl-dsa-perl, erlang, boinc-client, m2crypto	MLIST	openwall.com
#511515 - m2crypto: openssl return values. - Debian Bug report logs	MISC	bugs.debian.org
Bug 479676 – CVE-2009-0127 m2crypto: OpenSSL incorrect checks for malformed signatures	MISC	bugzilla.redhat.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Organization	Published	Contributor	Statement
Red Hat	2009-01-21	Tomas Hoger	Red Hat does not consider this to be a security issue. M2Crypto provides python interfaces to r

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](#)