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, ECDS

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-llnl, libnasl, libcrypt-openssl-dsa-perl, erlang, boinc-client, m2crypto	MLIST	openwall.com
#511515 - m2crypto: openssl return values. - Debian Bug report logs	MISC	bugs.debian.o
Bug 479676 – CVE-2009-0127 m2crypto: OpenSSL incorrect checks for malformed signatures	MISC	bugzilla.redhat
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.

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**