



CVE-2009-0124

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

Summary

CVE	CVE-2009-0124
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-01-15 17:30:00 UTC
Updated	2009-02-06 07:05:00 UTC
Description	The tqslib_verifyDataBlock function in openssl_cert.cpp in American Radio Relay League (ARRL) tqsllib 2.0 does not properly

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Arrl	Tqsllib	2.0	All	All	All
Application	Arrl	Tqsllib	2.0	All	All	All

References

Reference	Source	Link
oss-security - CVE Request -- tqsllib, slurml-lnl, libnasl, libcrypt-openssl-dsa-perl, erlang, boinc-client, m2crypto	MLIST	openwall.com
Fedora update for tqsllib - Secunia.com	SECUNIA	secunia.com
[SECURITY] Fedora 9 Update: tqsllib-2.0-5.fc9	FEDORA	www.redhat.cc
#511509 - tqsllib: Improper checking of the return value of EVP_VerifyFinal() - Debian Bug report logs	MISC	bugs.debian.o
Bug 479650 – CVE-2009-0124 tqsllib: OpenSSL incorrect checks for malformed signatures	CONFIRM	bugzilla.redhat
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](#)