



CVE-2014-9424

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

Summary

CVE	CVE-2014-9424
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-12-29 00:59:00 UTC
Updated	2014-12-30 15:35:00 UTC
Description	Double free vulnerability in the ssl_parse_clienthello_use_srtp_ext function in d1_srtp.c in LibreSSL before 2.1.2 allows remote attackers to cause a denial of service (crash) via crafted TLS records.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openbsd	Libressl	All	All	All	All

References

Reference	Source	Link
Issue 202 - google-security-research - LibreSSL DTLS double free - Google Security Research - Google Project Hosting	MISC	code.
Avoid a double-free in an error path. · robertbachmann/openbsd-libssl@62a110d · GitHub	CONFIRM	github
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)