CVE-2017-8301

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2017-8301
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-04-27 17:59:00 UTC
Updated	2019-10-03 00:03:00 UTC
Description	LibreSSL 2.5.1 to 2.5.3 lacks TLS certificate verification if SSL_get_verify_result is relied upon for a later check of a verifica

Risk And Classification

Problem Types: CWE-295

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openbsd	Libressl	2.5.1	All	All	All
Application	Openbsd	Libressl	2.5.2	All	All	All
Application	Openbsd	Libressl	2.5.3	All	All	All
Application	Openbsd	Libressl	2.5.1	All	All	All
Application	Openbsd	Libressl	2.5.2	All	All	All
Application	Openbsd	Libressl	2.5.3	All	All	All

References

Reference	Source	L
oss-sec: CVE-2017-8301: TLS verification vulnerability in LibreSSL 2.5.1 - 2.5.3	MISC	s
LibreSSL CVE-2017-8301 Certificate Validation Security Bypass Vulnerability	BID	w
Some nginx TLS tests started failing with LibreSSL 2.5.3 (but not with 2.4.4) · Issue #307 · libressl-portable/portable · GitHub	CONFIRM	g
#1257 (Some nginx TLS tests started failing with LibreSSL 2.5.3) – nginx	CONFIRM	tr
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500367 Alpine Linux Security Update for libressl