CVE-2013-4623

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2013-4623
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-09-30 22:55:00 UTC
Updated	2013-10-31 03:35:00 UTC
Description	The x509parse_crt function in x509.h in PolarSSL 1.1.x before 1.1.7 and 1.2.x before 1.2.8 does not properly parse certifica

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Polarssl	Polarssl	1.1.0	All	All	All
Application	Polarssl	Polarssl	1.1.0	rc0	All	All
Application	Polarssl	Polarssl	1.1.0	rc1	All	All
Application	Polarssl	Polarssl	1.1.1	All	All	All
Application	Polarssl	Polarssl	1.1.2	All	All	All
Application	Polarssl	Polarssl	1.1.3	All	All	All
Application	Polarssl	Polarssl	1.1.4	All	All	All
Application	Polarssl	Polarssl	1.1.5	All	All	All
Application	Polarssl	Polarssl	1.1.6	All	All	All
Application	Polarssl	Polarssl	1.2.0	All	All	All
Application	Polarssl	Polarssl	1.2.1	All	All	All
Application	Polarssl	Polarssl	1.2.2	All	All	All
Application	Polarssl	Polarssl	1.2.3	All	All	All
Application	Polarssl	Polarssl	1.2.4	All	All	All
Application	Polarssl	Polarssl	1.2.5	All	All	All
Application	Polarssl	Polarssl	1.2.6	All	All	All
Application	Polarssl	Polarssl	1.2.7	All	All	All

Application	Polarssl	Polarssl	1.1.0	All	All	All
Application	Polarssl	Polarssl	1.1.0	rc0	All	All
Application	Polarssl	Polarssl	1.1.0	rc1	All	All
Application	Polarssl	Polarssl	1.1.1	All	All	All
Application	Polarssl	Polarssl	1.1.2	All	All	All
Application	Polarssl	Polarssl	1.1.3	All	All	All
Application	Polarssl	Polarssl	1.1.4	All	All	All
Application	Polarssl	Polarssl	1.1.5	All	All	All
Application	Polarssl	Polarssl	1.1.6	All	All	All
Application	Polarssl	Polarssl	1.2.0	All	All	All
Application	Polarssl	Polarssl	1.2.1	All	All	All
Application	Polarssl	Polarssl	1.2.2	All	All	All
Application	Polarssl	Polarssl	1.2.3	All	All	All
Application	Polarssl	Polarssl	1.2.4	All	All	All
Application	Polarssl	Polarssl	1.2.5	All	All	All
Application	Polarssl	Polarssl	1.2.6	All	All	All
Application	Polarssl	Polarssl	1.2.7	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-2782-1 polarssl	DEBIAN	www.de
PolarSSL Security Advisory 2013-03 - Tech Updates	CONFIRM	polarssl
ssl_parse_certificate() now calls x509parse_crt_der() directly · ARMmbed/mbedtls@1922a4e · GitHub	CONFIRM	github.c
[SECURITY] Fedora 18 Update: polarssl-1.2.8-1.fc18	FEDORA	lists.fed
[SECURITY] Fedora 19 Update: polarssl-1.2.8-1.fc19	FEDORA	lists.fed
Bug 997767 – CVE-2013-4623 polarssl: denial of service (infinite loop) when parsing certain PEM encoded certificates	CONFIRM	bugzilla
[SECURITY] Fedora 20 Update: polarssl-1.2.8-1.fc20	FEDORA	lists.fed
PolarSSL Certificate Message Remote Denial of Service Vulnerability	BID	www.se
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nist

No vendor comments have been submitted for this CVE.

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