CVE-2013-1621

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2013-1621
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-08 19:55:00 UTC
Updated	2013-03-08 04:12:00 UTC
Description	Array index error in the SSL module in PolarSSL before 1.2.5 might allow remote attackers to cause a denial of service via

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Polarssl	Polarssl	0.10.0	All	All	All
Application	Polarssl	Polarssl	0.10.1	All	All	All
Application	Polarssl	Polarssl	0.11.0	All	All	All
Application	Polarssl	Polarssl	0.11.1	All	All	All
Application	Polarssl	Polarssl	0.12.0	All	All	All
Application	Polarssl	Polarssl	0.12.1	All	All	All
Application	Polarssl	Polarssl	0.13.1	All	All	All
Application	Polarssl	Polarssl	0.14.0	All	All	All
Application	Polarssl	Polarssl	0.14.2	All	All	All
Application	Polarssl	Polarssl	0.14.3	All	All	All
Application	Polarssl	Polarssl	0.99	pre1	All	All
Application	Polarssl	Polarssl	0.99	pre3	All	All
Application	Polarssl	Polarssl	0.99	pre4	All	All
Application	Polarssl	Polarssl	0.99	pre5	All	All
Application	Polarssl	Polarssl	1.0.0	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	1.2.0	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	0.10.0	All	All	All
Application	Polarssl	Polarssl	0.10.1	All	All	All
Application	Polarssl	Polarssl	0.11.0	All	All	All
Application	Polarssl	Polarssl	0.11.1	All	All	All
Application	Polarssl	Polarssl	0.12.0	All	All	All
Application	Polarssl	Polarssl	0.12.1	All	All	All
Application	Polarssl	Polarssl	0.13.1	All	All	All
Application	Polarssl	Polarssl	0.14.0	All	All	All
Application	Polarssl	Polarssl	0.14.2	All	All	All
Application	Polarssl	Polarssl	0.14.3	All	All	All
Application	Polarssl	Polarssl	0.99	pre1	All	All
Application	Polarssl	Polarssl	0.99	pre3	All	All
Application	Polarssl	Polarssl	0.99	pre4	All	All
Application	Polarssl	Polarssl	0.99	pre5	All	All
Application	Polarssl	Polarssl	1.0.0	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	1.2.0	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	All	All	All	All

References

Reference	Source	Link	Tag
PolarSSL 1.2.5 released - Tech Updates	CONFIRM	polarssl.org	Pat
Debian -- Security Information -- DSA-2622-1 polarssl	DEBIAN	www.debian.org	
oss-security - Re: CVE request: TLS CBC padding timing flaw in various SSL / TLS implementations	MLIST	openwall.com	
www.isg.rhul.ac.uk/tls/TLStiming.pdf	MISC	www.isg.rhul.ac.uk	
CVE Program record	CVE.ORG	www.cve.org	can
NVD vulnerability detail	NVD	nvd.nist.gov	can

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 registred 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