



# CVE-2013-4623

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2013-4623
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2013-09-30 22:55:00 UTC
<b>Updated</b>	2013-10-31 03:35:00 UTC
<b>Description</b>	The x509parse_cert 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 certificate

## 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	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.1.0	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.1.0	rc0	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.1.0	rc1	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.1.1	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.1.2	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.1.3	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.1.4	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.1.5	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.1.6	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.2.0	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.2.1	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.2.2	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.2.3	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.2.4	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.2.5	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.2.6	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.2.7	All	All	All

## References

Reference	Source	Link
Debian -- Security Information -- DSA-2782-1 polarssl	DEBIAN	<a href="#">www.de</a>
PolarSSL Security Advisory 2013-03 - Tech Updates	CONFIRM	<a href="#">polarssl</a>
ssl_parse_certificate() now calls x509parse_cert_der() directly · ARMmbed/mbedtls@1922a4e · GitHub	CONFIRM	<a href="#">github.c</a>
[SECURITY] Fedora 18 Update: polarssl-1.2.8-1.fc18	FEDORA	<a href="#">lists.fed</a>
[SECURITY] Fedora 19 Update: polarssl-1.2.8-1.fc19	FEDORA	<a href="#">lists.fed</a>
Bug 997767 – CVE-2013-4623 polarssl: denial of service (infinite loop) when parsing certain PEM encoded certificates	CONFIRM	<a href="#">bugzilla</a>
[SECURITY] Fedora 20 Update: polarssl-1.2.8-1.fc20	FEDORA	<a href="#">lists.fed</a>
PolarSSL Certificate Message Remote Denial of Service Vulnerability	BID	<a href="#">www.se</a>
CVE Program record	CVE.ORG	<a href="#">www.cv</a>
NVD vulnerability detail	NVD	<a href="#">nvd.nist</a>

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](#).

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