



# CVE-2014-8627

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

## Summary

<b>CVE</b>	CVE-2014-8627
<b>State</b>	PUBLIC
<b>Assigner</b>	security@suse.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-11-24 15:59:00 UTC
<b>Updated</b>	2023-11-07 02:22:00 UTC
<b>Description</b>	PolarSSL 1.3.8 does not properly negotiate the signature algorithm to use, which allows remote attackers to conduct downc

## Risk And Classification

**Problem Types:** CWE-310

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.3.8	All	All	All
Application	<a href="#">Polarssl</a>	<a href="#">Polarssl</a>	1.3.8	All	All	All

## References

Reference	Source	Link	Tags
PolarSSL 1.3.9 released - Tech Updates	CONFIRM	<a href="#">polarssl.org</a>	Patch, Vendor A
openSUSE-SU-2014:1457-1: moderate: Security update for polarssl		<a href="#">lists.opensuse.org</a>	
Security Advisory SA61220 - PolarSSL Security Issue and Two Vulnerabilities - Secunia		<a href="#">secunia.com</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonical, analy

No vendor comments have been submitted for this CVE.

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

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](#)**