CVE-2013-5915

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2013-5915
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-10-04 17:55:00 UTC
Updated	2013-10-31 03:35:00 UTC
Description	The RSA-CRT implementation in PolarSSL before 1.2.9 does not properly perform Montgomery multiplication, which might

Risk And Classification

Problem Types: CWE-310

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	1.1.6	All	All	All
Application	Polarssl	Polarssl	1.1.8	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	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	1.1.6	All	All	All
Application	Polarssl	Polarssl	1.1.8	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	All	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-2782-1 polarssl	DEBIAN	www.debian.org	
98049	OSVDB	osvdb.org	
Security Advisory SA55084 - PolarSSL RSA Private Key Recovery Weakness - Secunia	SECUNIA	secunia.com	Vendor Adv
PolarSSL Security Advisory 2013-05 - Tech Updates	CONFIRM	polarssl.org	Vendor Adv
[SECURITY] Fedora 18 Update: polarssl-1.2.9-1.fc18	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 19 Update: polarssl-1.2.9-1.fc19	FEDORA	lists.fedoraproject.org	
[SECURITY] Fedora 20 Update: polarssl-1.2.9-1.fc20	FEDORA	lists.fedoraproject.org	
PolarSSL RSA Private Key Recovery Security Bypass Vulnerability	BID	www.securityfocus.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, a

No vendor comments have been submitted for this CVE.

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

CVE.report and Source URL Uptime Status status.cve.report