CVE-2013-1623

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2013-1623
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-02-08 19:55:00 UTC
Updated	2014-02-21 04:58:00 UTC
Description	The TLS and DTLS implementations in wolfSSL CyaSSL before 2.5.0 do not properly consider timing side-channel attacks

Risk And Classification

Problem Types: CWE-310

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Yassl	Cyassl	0.2.0	All	All	All
Application	Yassl	Cyassl	0.3.0	All	All	All
Application	Yassl	Cyassl	0.4.0	All	All	All
Application	Yassl	Cyassl	0.5.0	All	All	All
Application	Yassl	Cyassl	0.5.5	All	All	All
Application	Yassl	Cyassl	0.6.0	All	All	All
Application	Yassl	Cyassl	0.6.2	All	All	All
Application	Yassl	Cyassl	0.6.3	All	All	All
Application	Yassl	Cyassl	0.8.0	All	All	All
Application	Yassl	Cyassl	0.9.0	All	All	All
Application	Yassl	Cyassl	0.9.6	All	All	All
Application	Yassl	Cyassl	0.9.8	All	All	All
Application	Yassl	Cyassl	0.9.9	All	All	All
Application	Yassl	Cyassl	1.0.0	rc1	All	All
Application	Yassl	Cyassl	1.0.0	rc2	All	All
Application	Yassl	Cyassl	1.0.0	rc3	All	All
Application	Yassl	Cyassl	1.0.2	All	All	All

Application	Yassl	Cyassl	1.0.3	All	All	All
Application	Yassl	Cyassl	1.0.6	All	All	All
Application	Yassl	Cyassl	1.1.0	All	All	All
Application	Yassl	Cyassl	1.2.0	All	All	All
Application	Yassl	Cyassl	1.3.0	All	All	All
Application	Yassl	Cyassl	1.4.0	All	All	All
Application	Yassl	Cyassl	1.5.0	All	All	All
Application	Yassl	Cyassl	1.5.4	All	All	All
Application	Yassl	Cyassl	1.5.6	All	All	All
Application	Yassl	Cyassl	1.6.0	All	All	All
Application	Yassl	Cyassl	1.6.5	All	All	All
Application	Yassl	Cyassl	1.8.0	All	All	All
Application	Yassl	Cyassl	1.9.0	All	All	All
Application	Yassl	Cyassl	2.0.0	rc1	All	All
Application	Yassl	Cyassl	2.0.0	rc2	All	All
Application	Yassl	Cyassl	2.0.0	rc3	All	All
Application	Yassl	Cyassl	2.0.2	All	All	All
Application	Yassl	Cyassl	2.0.6	All	All	All
Application	Yassl	Cyassl	2.0.8	All	All	All
Application	Yassl	Cyassl	2.2.0	All	All	All
Application	Yassl	Cyassl	2.3.0	All	All	All
Application	Yassl	Cyassl	2.4.0	All	All	All
Application	Yassl	Cyassl	0.2.0	All	All	All
Application	Yassl	Cyassl	0.3.0	All	All	All
Application	Yassl	Cyassl	0.4.0	All	All	All
Application	Yassl	Cyassl	0.5.0	All	All	All
Application	Yassl	Cyassl	0.5.5	All	All	All
Application	Yassl	Cyassl	0.6.0	All	All	All
Application	Yassl	Cyassl	0.6.2	All	All	All
Application	Yassl	Cyassl	0.6.3	All	All	All
Application	Yassl	Cyassl	0.8.0	All	All	All
Application	Yassl	Cyassl	0.9.0	All	All	All
Application	Yassl	Cyassl	0.9.6	All	All	All
Application	Yassl	Cyassl	0.9.8	All	All	All
Application	Yassl	Cyassl	0.9.9	All	All	All

Application	Yassl	Cyassl	1.0.0	rc1	All	All
Application	Yassl	Cyassl	1.0.0	rc2	All	All
Application	Yassl	Cyassl	1.0.0	rc3	All	All
Application	Yassl	Cyassl	1.0.2	All	All	All
Application	Yassl	Cyassl	1.0.3	All	All	All
Application	Yassl	Cyassl	1.0.6	All	All	All
Application	Yassl	Cyassl	1.1.0	All	All	All
Application	Yassl	Cyassl	1.2.0	All	All	All
Application	Yassl	Cyassl	1.3.0	All	All	All
Application	Yassl	Cyassl	1.4.0	All	All	All
Application	Yassl	Cyassl	1.5.0	All	All	All
Application	Yassl	Cyassl	1.5.4	All	All	All
Application	Yassl	Cyassl	1.5.6	All	All	All
Application	Yassl	Cyassl	1.6.0	All	All	All
Application	Yassl	Cyassl	1.6.5	All	All	All
Application	Yassl	Cyassl	1.8.0	All	All	All
Application	Yassl	Cyassl	1.9.0	All	All	All
Application	Yassl	Cyassl	2.0.0	rc1	All	All
Application	Yassl	Cyassl	2.0.0	rc2	All	All
Application	Yassl	Cyassl	2.0.0	rc3	All	All
Application	Yassl	Cyassl	2.0.2	All	All	All
Application	Yassl	Cyassl	2.0.6	All	All	All
Application	Yassl	Cyassl	2.0.8	All	All	All
Application	Yassl	Cyassl	2.2.0	All	All	All
Application	Yassl	Cyassl	2.3.0	All	All	All
Application	Yassl	Cyassl	2.4.0	All	All	All
Application	Yassl	Cyassl	All	All	All	All

References

Reference	Source	Li
About Secunia Research | Flexera	SECUNIA	se
wolfSSL, provider of CyaSSL Embedded SSL, releases first embedded TLS and DTLS protocol fix for Lucky Thirteen Attack	CONFIRM	w
Gentoo Linux Documentation -- MySQL: Multiple vulnerabilities	GENTOO	se
oss-security - Re: CVE request: TLS CBC padding timing flaw in various SSL / TLS implementations	MLIST	op
www.isg.rhul.ac.uk/tls/TLStiming.pdf	MISC	w
CVE Program record	CVE.ORG	w

NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

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