



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

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](#).

Free CVE JSON API [cve.report/api](#)

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