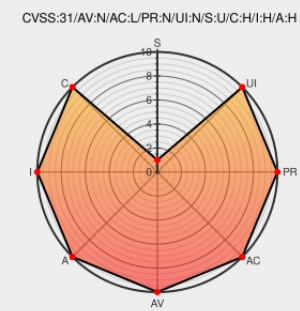
CVE-2014-2897

Published on: 01/28/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:58 PM UTC

CVE-2014-2897

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wolfssl from Wolfssl contain the following vulnerability:

The SSL 3 HMAC functionality in wolfSSL CyaSSL 2.5.0 before 2.9.4 does not check the padding length when verification fails, which allows remote attackers to have unspecified impact via a crafted HMAC, which triggers an out-of-bounds read.

CVE-2014-2897 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
wolfSSL Security Advisory: April 9, 2014 - wolfSSL	Vendor Advisory, www.wolfssl.com, text/html	CONFIRM www.wolfssl.com/yaSSL/Blog/Entries/2014/4/11_wolfSSL_Security_Advisory__April_9%2C_2014.html

oss-sec: CVE ids for CyaSSL 2.9.4?	Mailing List Third Party Advisory seclists.org text/html	MISC seclists.org/oss-sec/2014/q2/126
wolfSSL - Docs | CyaSSL ChangeLog	Vendor Advisory www.wolfssl.com text/xml	CONFIRM www.wolfssl.com/yaSSL/Docs-cyassl-changelog.html
oss-sec: Re: CVE ids for CyaSSL 2.9.4?	Mailing List Third Party Advisory seclists.org text/html	MISC seclists.org/oss-sec/2014/q2/130

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wolfssl	Wolfssl	All	All	All	All
Application	Wolfssl	Wolfssl	All	All	All	All

cpe:2.3:a:wolfssl:wolfssl:*:*:*:*:*:*:*:*:

cpe:2.3:a:wolfssl:wolfssl:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→