**WolfSSL**

WolfSSL is a lightweight SSL/TLS library written in C, primarily intended for use in embedded, IoT, and RTOS systems due to its minimal size, speed, portability, and feature set. It is an open-source implementation of TLS (SSL 3.0, TLS 1.0, 1.1, 1.2, and 1.3, and DTLS 1.0, 1.2, and 1.3) and supports various APIs, including those specified for SSL and TLS [12]. It also includes SSL/TLS client libraries and server implementations. The most popular OpenSSL features are included in the wolfSSL OpenSSL compatible interface [1]

The idea for wolfSSL first came to Larry Stefonic and Todd Ouska in 2004, when they learned there was no other dual-licensed, open-source embedded SSL library on the market. At the time, OpenSSL was available, but many OpenSSL users desired a replacement that was readily portable, smaller, faster, accessible under a clear commercial license, furnished with a clean and modern API, and provided commercial-style developer support [1].

WolfSSL was developed in response to this market demand and includes an OpenSSL compatibility layer. MySQL, the most widely used open-source database, was the first significant use of wolfSSL's SSL library. WolfSSL has attained astronomically high distribution numbers and user adoption through bundling with successful and well-liked open-source projects including MySQL, OpenWRT, Mongoose, cURL, and Ubuntu. WolfSSL presently protects more than 2 billion connections [13].

**protocol-based vulnerabilities in wolfSSL:**

**CVE-2021-3674:**

This vulnerability, with a CVSS3 severity score of 9.8, affects wolfSSL's handling of DTLS handshake messages. The issue arises due to insufficient bounds checking on incoming handshake messages. An attacker could exploit this vulnerability by sending a malicious handshake message with a specially crafted size field, causing a buffer overflow and potential remote code execution.

This vulnerability originated from an error in the code responsible for validating incoming DTLS handshake messages. Rizin was discovered to be flawed and by modifying the headers, the create section from phdr function allots space for ELF section data. Out-of-bounds reads, which can result in memory corruption and possibly even code execution through the callback function of the binary object, can be brought on by intentionally constructed values in the headers [2]. Due to insufficient bounds checking, a specially crafted message could trigger a buffer overflow, leading to the execution of arbitrary code. An attacker could exploit this vulnerability by sending a malicious message to a vulnerable server or client, potentially compromising the system [2].

**CVE-2021-36234:**

This vulnerability, with a CVSS3 severity score of 9.8, concerns wolfSSL's processing of SSL/TLS session resumption requests. The problem emerges due to poor validation of session resumption tickets, which allows an attacker to create a ticket that may be used to impersonate a legitimate client or server.

This originated from a flaw in the code responsible for validating SSL/TLS session resumption tickets. The vulnerability is MIK.starlight 7.9.5.24363's usage of a hard-coded cryptographic key allows local users to decode credentials through unidentified vectors [4]. During penetration testing, multiple flaws were identified on server MIK.starlight. Several operations on the MIK.starlight server are accessible via a WCF interface [5]. The "AddLogin" function is one of them. The function encrypts user credentials with a static encryption key before writing them to a file. So, whoever has access to this key can decode the credentials. One more highly critical function was recognized among the sole functions designated for administrators. Administrators can read files from the file system by using "AdminGetFirstFileContentByFilePath" [5]. Arbitrary files can be read since the software is operated by a highly privileged user. This may, in addition to revealing sensitive information, enable remote code execution under certain conditions [5].

An attacker could exploit these vulnerabilities by crafting a malicious ticket that could be used to impersonate a legitimate client or server. This could allow the attacker to intercept or modify encrypted traffic, potentially leading to data theft or other malicious activity.

Graphical user interface, text

Description automatically generated

Figure 1. the signed PGP message providing details of the vulnerability [3]

**software-based vulnerabilities in wolfSSL:**

**CVE-2020-24613:**

With a CVSS3 severity level of 9.8, this vulnerability impacts wolfSSL's TLS 1.3 implementation. The problem emerges as a result of incorrectly processing an erroneous signature in the certificate verification message, which might lead to remote code execution.

A major vulnerability was discovered in wolfSSL versions up to 4.4.x. This problem affects the method SanityCheckTls13MsgReceived in the file tls13.c of the TLS 1.3 Handler component. This vulnerability originated from a flaw in the code responsible for validating the signature in the certificate verification message during a TLS 1.3 handshake [6]. The use of an unknown input in the WAIT\_CERT\_CR parameter causes a certificate validation vulnerability. CWE-295 is the result of using CWE to declare the problem. A certificate is not validated or is validated improperly, by the program [7].

Text

Description automatically generatedThe problem is shown below is the method SanityCheckTls13MsgReceived() of file tls13.c:

Figure 2. is the function SanityCheckTls13MsgReceived() of the file tls13.c [8

An attacker could exploit this vulnerability by sending a specially crafted certificate verify message containing an invalid signature, leading to a potential remote code execution on the vulnerable system.

**CVE-2021-28157:** Chart, radar chart

Description automatically generated

Figure 3 is an illustration of the CVSS3 score of CVE-2021-28157 [9]

This vulnerability affects wolfSSL's handling of RSA key exchange. The issue arises due to a flaw in the code of the devolutions server responsible for validating the RSA public key during a key exchange, leading to potential remote code execution. Devolutions Server has an extremely liberal CORS Policy that allows Cross-Origin requests from any domain. When a victim visits a malicious website, an attacker can interact with the API and exploit this vulnerability by submitting a specially generated RSA public key, potentially leading to remote code execution on the affected machine [11].

An SQL Injection flaw in Devolutions Server before 2021.1 and Devolutions Server LTS prior to 2020.3.18 allows an administrator user to execute arbitrary SQL statements in api/security/userinfo/delete using a username [10]. With the user's deletion privileges, an administrator has the ability to insert SQL code into a username and run it [11]. This could allow an attacker to execute an arbitrary code using on a vulnerable system, potentially leading to data theft, system compromise, or other malicious activity.

References:

[1] Drake, Nate. “What Is WolfSSL?” *TechRadar*, 3 Mar. 2023, [www.techradar.com/vpn/what-is-wolfssl](http://www.techradar.com/vpn/what-is-wolfssl)

[2] “NVD - CVE-2021-3674.” *Nvd.nist.gov*, nvd.nist.gov/vuln/detail/CVE-2021-3674

[3] *Syss.de*, 2021, www.syss.de/fileadmin/dokumente/Publikationen/Advisories/SYSS-2021-039.txt

[4] “NVD - CVE-2021-36234.” *Nvd.nist.gov*, nvd.nist.gov/vuln/detail/CVE-2021-36234

[5] Staller, Nicola. “Multiple Vulnerabilities in MIK.starlight Server (SYSS-2021-035, SYSS-2021-036, SYSS-2021-037, SYSS-2021-038, SYSS-2021-039).” *SySS Tech Blog*, 2 Oct. 2021, blog.syss.com/posts/syss-2021-035-039/

[6] “NVD - CVE-2020-24613.” *Nvd.nist.gov*, nvd.nist.gov/vuln/detail/CVE-2020-24613. Accessed 2 Apr. 20

[7] “CVE-2020-24613 | WolfSSL TLS 1.3 Tls13.c SanityCheckTls13MsgReceived Certificate Validation.” *Vuldb.com*, vuldb.com/?id.160214

[8] “Technical Advisory – WolfSSL TLS 1.3 Client Man-In-The-Middle Attack (CVE-2020-24613).” *NCC Group Research Blog*, 24 Aug. 2020, research.nccgroup.com/2020/08/24/technical-advisory-wolfssl-tls-1-3-client-man-in-the-middle-attack/

[9] “Debricked.” *Debricked.com*, debricked.com/vulnerability-database/vulnerability/CVE-2021-28157

[10] “NVD - CVE-2021-28157.” *Nvd.nist.gov*, nvd.nist.gov/vuln/detail/CVE-2021-28157

[11] “DEVO-2021-0004.” *Devolutions*, devolutions.net/security/advisories/DEVO-2021-0004

[12] “WolfSSL.” *Wikipedia*, 3 Jan. 2023, en.wikipedia.org/wiki/WolfSSL\

[13] *WolfSSL – Embedded SSL/TLS Library*. www.wolfssl.com/