Buffer Overflow Due to Integer Underflow in Crypto_TC_Prep_AAD of CryptoLib

High **jlucas9** published **GHSA-q4v2-fvrv-qrf6** 5 days ago

Package	Affected versions	Patched versions
No package listed	<= 1.3.3	None

Severity

High

CVE ID

CVE-2025-29913

Weaknesses

CWE-125 CWE-191

Credits

mirkobitetto Finder

juriSacchetta Coordinator

danmaam Coordinator

Description

Summary

A critical heap buffer overflow vulnerability was identified in the `Crypto_TC_Prep_AAD` function of CryptoLib. This vulnerability allows an attacker to trigger a Denial of Service (DoS) or potentially execute arbitrary code (RCE) by providing a maliciously crafted telecommand (TC) frame that causes an unsigned integer underflow.

Details

The vulnerability lies in the function `Crypto_TC_Prep_AAD`, specifically during the computation of `tc_mac_start_index`. The affected code incorrectly calculates the MAC start index without ensuring it remains within the bounds of the `ingest` buffer. When `tc_mac_start_index` underflows due to an incorrect length calculation, the function attempts to access an out-of-bounds memory location, leading to a segmentation fault.

Vulnerable Code:

```
uint16_t tc_mac_start_index = tc_sdls_processed_frame->tc_header +

// Parse the received MAC
memcpy((tc_sdls_processed_frame->tc_sec_trailer.mac), &(ingest[tc_mac
```

Root Cause:

- The calculation of `tc_mac_start_index` can result in an underflow when `tc_sdls_processed_frame->tc_header.fl` is smaller than `fecf_len + sa_ptr->stmacf_len`.
- This leads to an out-of-bounds read when copying memory from `ingest`.

PoC

To reproduce the vulnerability, pass the following malicious packet to `Crypto_TC_ProcessSecurity`, which eventually calls `Crypto_TC_Prep_AAD`:

```
080300080B00000AE3B20E
```

The vulnerability is still present even in the latest commit of the advisory fix branch:
Commit: `d3cc420ace96d02a5b7e83d88cbd2e48010d5723`

ASan Output

The vulnerability was detected through AddressSanitizer (ASan), showing the following error:

```
==3369349==ERROR: AddressSanitizer: SEGV on unknown address
0x502000026f27 (pc 0x7beb3d77a322 bp 0x7ffe84148490 sp
0x7ffe84148428 T0)
==3369349==The signal is caused by a READ memory access.
    #0 0x7beb3d77a322  (/usr/lib/libc.so.6+0x16c322) (BuildId:
0b707b217b15b106c25fe51df3724b25848310c0)
    #1 0x7beb3e0ecc4b in Crypto_TC_Prep_AAD
/home/mirko/Downloads/CryptoLib-ghsa-q2pc-c3jx-3852-advisory-fix-
1/src/core/crypto_tc.c:1550
    #2 0x7beb3e0f1df0 in Crypto_TC_ProcessSecurity_Cam
/home/mirko/Downloads/CryptoLib-ghsa-q2pc-c3jx-3852-advisory-fix-
1/src/core/crypto_tc.c:1923
    #3 0x7beb3e0e92a1 in Crypto_TC_ProcessSecurity
/home/mirko/Downloads/CryptoLib-ghsa-q2pc-c3jx-3852-advisory-fix-
1/src/core/crypto_tc.c:1212
    #4 0x592ce8eee0b5 in main /home/mirko/Downloads/CryptoLib-
ghsa-q2pc-c3jx-3852-advisory-fix-1/test/core/apply_security.c:154
    #5 0x7beb3d635487  (/usr/lib/libc.so.6+0x27487) (BuildId:
0b707b217b15b106c25fe51df3724b25848310c0)
    #6 0x7beb3d63554b in __libc_start_main
(/usr/lib/libc.so.6+0x2754b) (BuildId:
0b707b217b15b106c25fe51df3724b25848310c0)
    #7 0x592ce8eed394 in _start (/home/mirko/Downloads/CryptoLib-
ghsa-q2pc-c3jx-3852-advisory-fix-1/build-
asan/test/test_apply_security+0x3394) (BuildId:
10a19f7cc5a279607e682d3f5cab92bc91ffc1eb)
```

Impact

- **Denial of Service (DoS)**: The application may crash due to the out-of-bounds memory access.
- **Remote Code Execution (RCE)**: If the overflow is exploited to manipulate the heap, arbitrary code execution may be possible.