Heap Buffer Overflow in Crypto_AOS_ProcessSecurity Function

High **jlucas9** published **GHSA-7g6g-9gj4-8c68** 5 days ago

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

Severity

High

CVE ID

CVE-2025-29911

Weaknesses

CWE-122

Credits

mirkobitetto Finder

danmaam Coordinator

juriSacchetta Coordinator

Description

Summary

A critical heap buffer overflow vulnerability was identified in the `Crypto_AOS_ProcessSecurity` 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 AOS frame with an insufficient length.

Details

The vulnerability lies in the function `Crypto_AOS_ProcessSecurity`, specifically during the processing of the Frame Error Control Field (FECF). The affected code attempts to read from the `p_ingest` buffer at indices `current_managed_parameters_struct.max_frame_size - 2` and `current_managed_parameters_struct.max_frame_size - 1` without verifying if `len_ingest` is sufficiently large. This leads to a heap buffer overflow when `len_ingest` is smaller than `max_frame_size`.

Vulnerable Code:

```
if (current_managed_parameters_struct.has_fecf == AOS_HAS_FECF)
{
    uint16_t received_fecf =
        (((p_ingest[current_managed_parameters_struct.max_frame_size
         (p_ingest[current_managed_parameters_struct.max_frame_size -
}
```

Root Cause:
The code does not validate `len_ingest` against `max_frame_size` before accessing the buffer, resulting in out-of-bounds memory access.

PoC

To reproduce the vulnerability, provide the following input to `Crypto_AOS_ProcessSecurity`:

```
char* test_aos_secured_h = "40303030303030303030FF35DF4008EF"; //
```

This input triggers an out-of-bounds read when `max_frame_size` is set to 1786 bytes.

ASan Output

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

```
==197671==ERROR: AddressSanitizer: heap-buffer-overflow on addr
0x502000017628 at pc 0x7caa86abcbde bp 0x7ffe85c3b930 sp
0x7ffe85c3b920
READ of size 1 at 0x502000017628 thread T0
#0 0x7caa86abcbdd in Crypto_AOS_ProcessSecurity
/home/mirko/Downloads/CryptoLib/src/core/crypto_aos.c:1082

#1 0x613c0ce1862f in main
```

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.