Talos Vulnerability Report

TALOS-2020-1174

FreyrSCADA IEC-60879-5-104 server simulator traffic logging denial-of-service vulnerability

JANUARY 11, 2021

CVE NUMBER

CVE--2020-13559

Summary

A denial-of-service vulnerability exists in the traffic-logging functionality of FreyrSCADA IEC-60879-5-104 Server Simulator 21.04.028. A specially crafted packet can lead to denial of service. An attacker can send a malicious packet to trigger this vulnerability.

Tested Versions

FreyrSCADA IEC-60879-5-104 Server Simulator 21.04.028

Product URLs

https://www.freyrscada.com/iec-60870-5-104.php

CVSSv3 Score

5.9 - CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

CWE

CWE-1024 - Comparison of Incompatible Types

Details

FreyrSCADA's IEC104 server simulator is a high-fidelity simulator built to the protocol specifications of IEC104. It is designed for the testing and development of IEC104-compliant tools and products.

Due to an incorrectly sized comparison within `FreryIEC104ServerSim.exe` a packet with size greater than 0xFF will cause a memory exhaustion denial of service due to an infinite loop when processing the packet for display within the simulator window.

This bug occurs when a packet's total size is greater than 1 byte (0xFF). This occurs due to a comparison between a word (2 bytes) and a byte (1 byte) to determine the end condition for a loop responsible for building a format string to display the packet contents within the Simulator window.

The max payload size of the packet is 0xFF, but 2 bytes are added to the length for the required header (0x68 and the byte that reports the length) thus creating an edgecase where the length of the packet can actually be up to 0x101 bytes. When this edge case occurs, the single byte loop index overflows before ever breaking the loop, resulting in an infinite loop. As the loop iterates, a string is being created, and memory is being allocated to fit it, after a large number of iterations, memory is exhausted and the program crashes.

```
00429aea 33c9 xor ecx, ecx {0x0}
// retrieve loop iteration
00429aec 8a4dc1 mov cl, byte [ebp-0x3f {loop_iteration}] <- Single byte loaded into cl
00429aef 8b450c mov eax, dword [ebp+0xc {packetLength}]
// Retrieve packet length
00429af2 0fb75008 movzx edx, word [eax+0x8] <- 2 bytes loaded and zero extended into edx
00429af6 3bca cmp ecx, edx <- ECX can never be greater than EDX, iff EDX is greater than 0xFF
// if loop_iteration > packetLength : break loop
00429af8 7cbf jl 0x429ab9
...
00429ab9 33c9 xor ecx, ecx {0x0}
00429abb 8a4dc1 mov cl, byte [ebp-0x3f {loop_iteration}]
00429abe 8b450c mov eax, dword [ebp+0xc {packetLength}]
00429ac1 33d2 xor edx, edx {0x0}
// get byte from packet data
00429ac3 8a94081a020000 mov dl, byte [eax+ecx+0x21a]
00429aca 52 push edx {var_50_5}
// %02x
00429acb 68b4887100 push data_7188b4 {var_54}
00429ad0 8d4df8 lea ecx, [ebp-0x8 {var_c}]
00429ad3 51 push ecx {var_c} {var_58_2}
00429ad4 e85bbd2c00 call sprintf
00429ad9 83c40c add esp, 0xc
00429adc 8d45fc lea eax, [ebp-0x4 {var_8}]
00429adf 8b55f8 mov edx, dword [ebp-0x8 {var_c}]
00429ae2 e83d860600 call append_data_to_string
00429ae7 fe45c1 inc byte [ebp-0x3f {loop_iteration}]
(loop back to 00429aea)
```

Crash Information

The resulting crash dump as a result of the infinite allocation loop is as follows:

```
(7404.216c): Unknown exception - code 0eedfade (first chance)
(7404.216c): Unknown exception - code 0eedfade (!!! second chance !!!)
eax=0c06f550 ebx=004a908b ecx=00000007 edx=00000000 esi=004a908b edi=00000000
eip=76dd9962 esp=0c06f550 ebp=0c06f5a8 iopl=0 nv up ei pl nz ac pe nc
cs=0023 ss=002b ds=002b es=002b fs=0053 gs=002b efl=00000216
KERNELBASE!RaiseException+0x62:
76dd9962 8b4c2454 mov ecx,dword ptr [esp+54h] ss:002b:0c06f5a4=9c39909d

[0x0] KERNELBASE!RaiseException + 0x62
[0x1] FreyrIEC104ServerSim!Unit7Finalize + 0x33f43
[0x2] IEC104!eCheckClientstatus + 0x34299
[0x3] IEC104!eCheckClientstatus + 0x34fb4
[0x4] IEC104!eCheckClientstatus + 0x34814
[0x5] IEC104!eCheckClientstatus + 0x340c3
```

Timeline

2020-10-26 - Vendor Disclosure

2020-01-05 - Follow up with vendor

2021-01-11 - Vendor patched; Public Release

CREDIT

Discovered by Jared Rittle of Cisco Talos.

VULNERABILITY REPORTS

PREVIOUS REPORT TALOS-2020-1163

NEXT REPORT TALOS-2020-1193