Talos Vulnerability Report

TALOS-2020-1170

EIP Stack Group OpENer Ethernet/IP server out-of-bounds write vulnerability

DECEMBER 2, 2020

CVE NUMBER

CVE-2020-13556

Summary

An out-of-bounds write vulnerability exists in the Ethernet/IP server functionality of EIP Stack Group OpENer 2.3 and development commit 8c73bf3. A specially crafted series of network requests can lead to remote code execution. An attacker can send a sequence of requests to trigger this vulnerability.

Tested Versions

EIP Stack Group OpENer 2.3
EIP Stack Group OpENer development commit 8c73bf3

Product URLs

https://github.com/EIPStackGroup/OpENer

CVSSv3 Score

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

CWE

CWE-787 - Out-of-bounds Write

Details

OpENer is an EtherNet/IP stack for I/O adapter devices. It supports multiple I/O and explicit connections and includes objects and services for making EtherNet/IP-compliant products as defined in the ODVA specification.

In file `source/src/enet_encap/cpf.c` there is a function `EipStatus CreateCommonPacketFormatStructure`.

The value `item_count` is read from the corresponding field in an ENIP packet, and used as a counter for a loop:

```
CipUint item_count = GetIntFromMessage(&data);
for (size_t j = 0; j < (common_packet_format_data->item_count - 2); j++) /* TODO there needs to be a limit check here???*/
    {
      common_packet_format_data->address_info_item[j].type_id =GetIntFromMessage(&data);
```

The `GetIntFromMessage` function reads two bytes and converts them to a short integer, which is written to an array inside the structure pointed by `common_packet_format_data`. This corresponds to the global variable `g_common_packet_format_data_item`.

If the `item_count` value is too big, the loop will read and write out of bounds, once it runs out of valid entrys in the `address_info_item` array. The out-of-bounds write starts from `g_common_packet_format_data_item` in the `.bss` segment and can overwrite the whole heap, which could lead to remote code execution.

Crash Information

GDB:

```
Starting program:
/home/wrl/opener-neu-20200814/OpENer-2.3/bin/posix/src/ports/POSIX/OpENer
ens33
[Thread debugging using libthread_db enabled]
Using host libthread_db library "/lib/x86_64-linux-gnu/libthread_db.so.1".

Program received signal SIGSEGV, Segmentation fault.
0x00005555555686df in CreateCommonPacketFormatStructure ()
(gdb) bt
 0  0x00005555555686df in CreateCommonPacketFormatStructure ()
 1  0x000055555556830a in NotifyConnectedCommonPacketFormat ()
 2  0x000055555556a698 in HandleReceivedSendUnitDataCommand ()
 3  0x00005555555697bb in HandleReceivedExplictTcpData ()
 4  0x000055555556cae6 in HandleDataOnTcpSocket ()
 5  0x000055555556bf68 in NetworkHandlerProcessOnce ()
 6  0x000055555555da32 in executeEventLoop ()
 7  0x000055555555d9e6 in main ()
(gdb) info registers
rax            0x55555559a008      93824992518152
rbx            0x55555556e1a0      93824992338336
rcx            0x0                 0
rdx            0x1b02              6914
rsi            0x5555555783c0      93824992379840
rdi            0x7fffffffdda8      140737488346536
rbp            0x7fffffffddd0      0x7fffffffddd0
rsp            0x7fffffffdd90      0x7fffffffdd90
r8             0x7fffffffdfb0      140737488347056
r9             0x7fffffffdfc0      140737488347072
r10            0x0                 0
r11            0x246               582
r12            0x55555555d700      93824992270080
r13            0x7fffffffe550      140737488348496
r14            0x0                 0
r15            0x0                 0
rip            0x5555555686df      0x5555555686df
<CreateCommonPacketFormatStructure+376>
eflags         0x10202             [ IF RF ]
cs             0x33                51
ss             0x2b                43
ds             0x0                 0
es             0x0                 0
fs             0x0                 0
gs             0x0                 0
```

Timeline

2020-08-18 - Vendor Disclosure

2020-10-22 - Follow up with vendor

2020-11-10 - Vendor confirmed issue under review

2020-12-02 - Vendor applied fix to master branch

2020-12-02 - Public Release

CREDIT

Discovered by Martin Zeiser of Cisco Talos.
