Talos Vulnerability Report

TALOS-2020-1143

EIP Stack Group OpENer ethernet/IP server denial-of-service vulnerability

DECEMBER 2, 2020

CVE NUMBER

CVE-2020-13530

Summary

A denial-of-service vulnerability exists in the Ethernet/IP server functionality of the EIP Stack Group OpENer 2.3 and development commit 8c73bf3. A large number of network requests in a small span of time can cause the running program to stop. 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

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

CWE

CWE-910 - Use of Expired File Descriptor

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.

Overloading the OpENer application with requests will result in a broken pipe, when it tries to reply to a socket that has already been closed.

The issue happens since the code does not handle signals of type `SIGPIPE`. In the `source/src/ports/` subdirectory, in file `generic_networkhandler.c`, the following `send()` call takes place in line 846:

```
datasent = send(socket, (char ) outgoingmessage.messagebuffer,
                      outgoingmessage.usedmessagelength, 0);
```

If the remote client has already closed the socket when OpENer tries to write to it, a SIGPIPE is triggered by the OS to the application, which results in OpENer being shut down due to the signal not being handled.

Crash Information

Strace output for the process:

```
select(7, [3 4 5 6], NULL, NULL, {tv_sec=0, tv_usec=6000}) = 1 (in [6],
left {tv_sec=0, tv_usec=5998})
recvfrom(6, "\276\357\0\0", 4, 0, NULL, NULL) = 4
recvfrom(6, "\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0", 20, 0, NULL,
NULL) = 20
getpeername(6, {sa_family=AF_INET, sin_port=htons(41382),
sin_addr=inet_addr("192.168.60.129")}, [16]) = 0
sendto(6, "\276\357\0\0\0\0\0\0\1\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0", 24, 0,
NULL, 0) = 24
select(7, [3 4 5 6], NULL, NULL, {tv_sec=0, tv_usec=5000}) = 1 (in [6],
left {tv_sec=0, tv_usec=4998})
recvfrom(6, "\276\357\0\0", 4, 0, NULL, NULL) = 4
recvfrom(6, "\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0", 20, 0, NULL,
NULL) = 20
getpeername(6, 0x7fff193d72a0, [16])    = -1 ENOTCONN (Transport
endpoint is not connected)
sendto(6, "\276\357\0\0\0\0\0\0\1\0\0\0\0\0\0\0\0\0\0\0\0\0\0\0", 24, 0,
NULL, 0) = -1 EPIPE (Broken pipe)
--- SIGPIPE {si_signo=SIGPIPE, si_code=SI_USER, si_pid=2072, si_uid=0} ---
+++ killed by SIGPIPE +++
```

Timeline

2020-08-18 - Vendor Disclosure
2020-10-22 - Follow up with vendor
2020-11-10 - Vendor confirmed issue under review
2020-11-30 - Vendor applied fix to master branch

2020-12-02 - Public Release

CREDIT

Discovered by Martin Zeiser and Jared Rittle of Cisco Talos.

© 2022 Cisco Systems, Inc. and/or its affiliates. All rights reserved. View our Privacy Policy.