# Omron Fins

*发表于 2021-01-25 更新于 2021-02-16 分类于 Challenge， 2020， 工业信息安全技能大赛， 哈尔滨站*
*Challenge | 2020 | 工业信息安全技能大赛 | 哈尔滨站 | Omron Fins*

*点击此处获得更好的阅读体验*

---

## *WriteUp来源*

*来自MO1N战队*

## *题目描述*

> *当通过 OMRON FINS-Tcp 协议向内存写入字符串数据时，会神奇的发现要写入的字符串数据在数据流量包中发生了改变，请根据协议特点分析出原始要写入的字符串数据。flag{string}*

## *题目考点*

- *流量分析*
- *OMRON FINS-Tcp读写数据不同内存区域数据的格式*
- *对Command Code掌握*
- *0x0101 - , "Memory Area Read*
- *0x0102 - Memory Area Write*
- *0x0103 - Memory Area Fill*
- *0x0104 - Multiple Memory Area Read*

## *解题思路*

*OMRON FINS-Tcp 向地址为D100字符串写入数据：qabd2twp970mdikt38*

### *流量分析*

*wireshark抓取流量包*

```
1 0000  50  e0  85  40  51  b9  a0  a4  c5  d9  ec  9d  08  00  45  00  P..@Q  E.
2 0010  00  5c  26  37  40  00  80  06  4d  99  c0  a8  02  c3  c0  a8  .\&7@...M.......
3 0020  02  b8  40  09  25  80  f6  21  29  39  cb  bd  9c  e7  50  18  ..@.%..!)9  P.
4 0030  40  14  96  ad  00  00  46  49  4e  53  00  00  00  2c  00  00  @.....FINS...,..
5 0040  00  02  00  00  00  00  80  00  02  00  01  00  00  c0  00  00  ................
6 0050  01  02  82  00  64  00  00  09  61  71  64  62  74  32  70  77  ....d...aqdbt2pw
7 0060  37  39  6d  30  69  64  74  6b  38  33                79m0idtk83
```

### *解析协议*

```
1 FINS/TCP帧(16bytes):          46  49 4e  53 00 00 00 2c 00  00 00 02 00 00 00 00
2 FINS UDP/IP帧(10bytes):       80  00 02  00 01 00 00 c0 00  00
3 command format:
4           Command code:       01  02
5           Memory area code:   82
6           Beginning address:  00  64 00
7           No. of items:       00  09
8           data:               61  71 64 62 74 32 70 77 37 39 6d 30 69 64 74 6b 38
9                               aqdbt2pw79m
```

*此时可以发现，流量包中的data数据 aqdbt2pw79m0idtk83与写入的 qabd2twp970mdikt38 数据不一致，这是因为写入的内存区域 Data 类型为Word contents*

如下图：

**Word contents**的格式为：

每个数据单元为2字节：第一字节：高8位，第二字节:低8位.如下图：

所以 qabd2twp970mdikt38字符串写入内存后为 aqdbt2pw79m0idtk83

## Omron Fins协议详解

Omron Fins-Tcp是一个FINS/TCP头部(必选)，加上FINS/UDP报文(可选)

```
1            Fins over TCP
2  +--------------------------------+
3  |        Fins/TCP Header         | (16 Bytes)
4  +--------------------------------+
5  |    UDP/IP 帧 (not neccessary)  | (10 Bytes)
6  +--------------------------------+
7  | command format(not neccessary) |
8  +--------------------------------+
9
10
11           Fins/TCP Header(16bytes)
12 0                                        31
13 +----------------------------------------+
14 |               Magic Bytes              | (4bytes)
15 +----------------------------------------+
16 |                  Length                | (4bytes)
17 +----------------------------------------+
18 |                  Command               | (4bytes)
19 +----------------------------------------+
20 |               Error Code               | (4bytes)
21 +----------------------------------------+
22 Magic Bytes (4bytes)    其ASCII码(0x46494E53)刚好是FINS
23 Length      (4bytes)    Length = len(TCP_PAYLOAD) - len(MagicBytes) - len(Length)
24                                = len(TCP_PAYLOAD) - 4 - 4
25                                = len(TCP_PAYLOAD) - 8
26 Command     (4bytes)
27 Error
```

```
1  UDP/IP 帧格式(10 Bytes):
2      ICF、RSV、GCT、DNA、DA1、DA2、SNA、SA1、SA2、SID
3          ICF 发送接收标志字节， 发送报文：0x80; 响应报文：0xc0 RSV 固定为 00
4          GCT 固 定 为 02 DNA 目标网络号： 本地 00
5          远程  01-7F
6          DA1 目标节点号
7          DA2 目标单元号
8          对CPU来说，固定为 00 SNA 源网络号
9          SA1 源节点号
10         SA2 原单元号
11         SID 服务ID
12 command format:
13     Command code:(2 Bytes)
14         { 0x0101, "Memory Area Read" },
15         { 0x0102, "Memory Area Write" },
16         { 0x0103, "Memory Area Fill" },
17         { 0x0104, "Multiple Memory Area Read" }
18     Memory area code     (1 Byte)
19     Beginning address    (3 Bytes)
20     No. of items         (2 Bytes)
21     Data:                (读写数据长度)
```

## 相关知识点

命令格式： 01+02+1字节存储区代码+3字节开始地址+2字节数量+第1字值+第2字值

# Flag

```
1 flag{qabd2twp970mdikt38}
```



# Challenge # 2020 # 工业信息安全技能大赛 # 哈尔滨站

BACnet

车间网络恶意攻击分析