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

OS-S Security Advisory 2017-02

Date: April 4th, 2017

Updated: April 12th, 2017

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

CVE: CVE-2017-7574

Vendor Reference: SEVD-2017-097-02

Vendor Advisory: http://www.schneider-electric.com/en/download/document/SEVD-2017-097-02/

CVSS: 10

Affected Device: Schneider SoMachine Basic 1.4 SP1, Schneider Modicon TM221CE16R, Firmware 1.3.3.3

Title: The password for the project protection of the Schneider Modicon TM221CE16R is hard-coded and cannot be changed.

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

Ease of Exploitation: Trivial

Vulnerability type: Information Disclosure

Vendor contacted: December 23rd, 2016

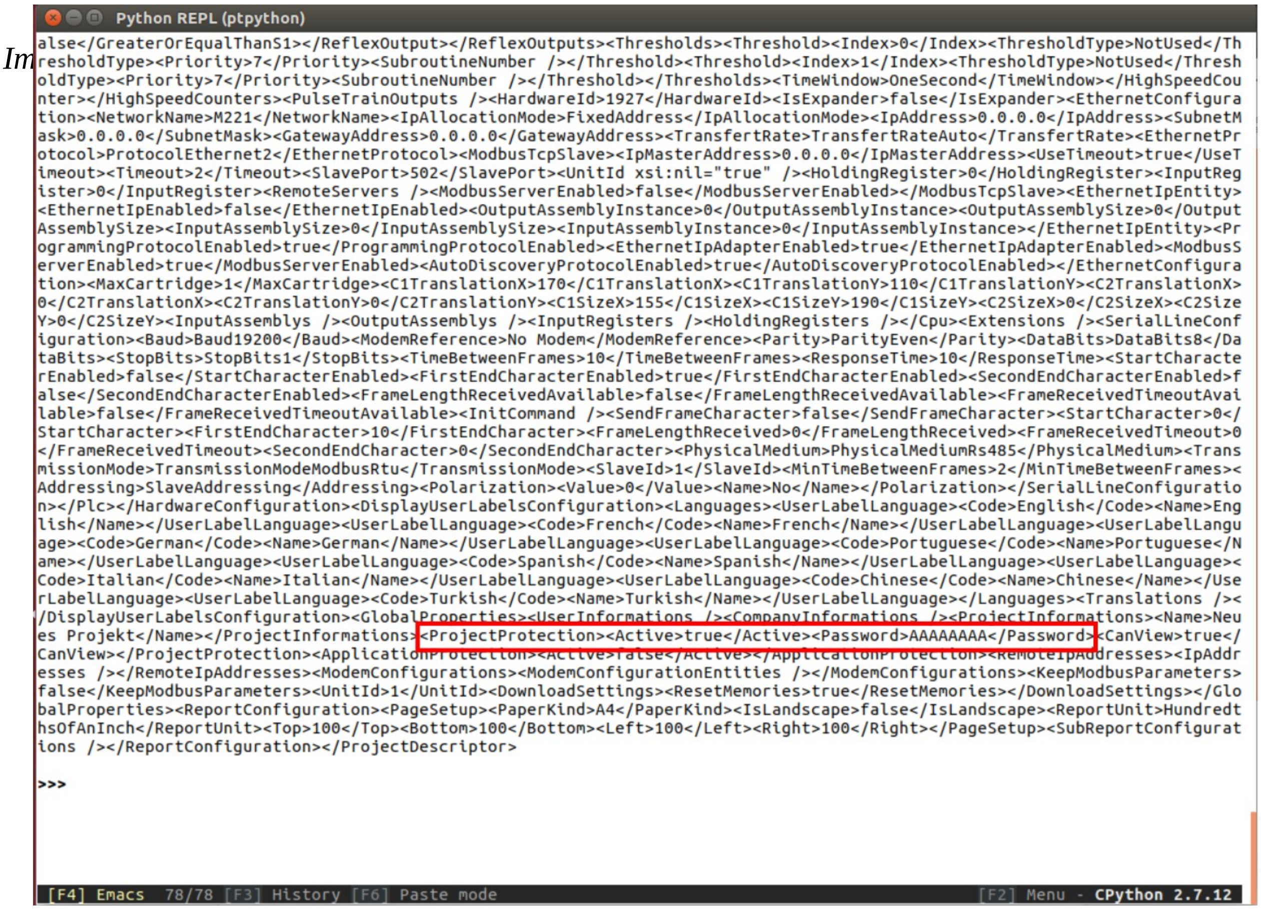
Abstract

The Project Protection is used to prevent unauthorized users from opening the protected project file by prompting the user for a password. The XML file is AES-CBC encrypted, however the key used for encryption is hard coded and cannot be changed. The key used for encryption is: **“SoMachineBasicSoMachineBasicSoMa”**. After decrypting the XML file with the standard password the user password can be found in the decrypted data. After reading the user password the project can be opened and modified with SoMachine Basic.

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 7th, 2017. The vendor will provide an update on June 15th 2017.

Im



Python REPL (ptpython)

```
alse</GreaterOrEqualThanS1></ReflexOutput></ReflexOutputs><Thresholds><Threshold><Index>0</Index><ThresholdType>NotUsed</Th
resholdType><Priority>7</Priority><SubroutineNumber /></Threshold><Threshold><Index>1</Index><ThresholdType>NotUsed</Thresh
oldType><Priority>7</Priority><SubroutineNumber /></Threshold></Thresholds><TimeWindow>OneSecond</TimeWindow></HighSpeedCou
nter></HighSpeedCounters><PulseTrainOutputs /><HardwareId>1927</HardwareId><IsExpander>false</IsExpander><EthernetConfigura
tion><NetworkName>M221</NetworkName><IpAllocationMode>FixedAddress</IpAllocationMode><IpAddress>0.0.0.0</IpAddress><SubnetM
ask>0.0.0.0</SubnetMask><GatewayAddress>0.0.0.0</GatewayAddress><TransfertRate>TransfertRateAuto</TransfertRate><EthernetPr
otocol>ProtocolEthernet2</EthernetProtocol><ModbusTcpSlave><IpMasterAddress>0.0.0.0</IpMasterAddress><UseTimeout>true</UseT
imeout><Timeout>2</Timeout><SlavePort>502</SlavePort><UnitId xsi:nil="true" /><HoldingRegister>0</HoldingRegister><InputReg
ister>0</InputRegister><RemoteServers /><ModbusServerEnabled>false</ModbusServerEnabled></ModbusTcpSlave><EthernetIpEntity>
<EthernetIpEnabled>false</EthernetIpEnabled><OutputAssemblyInstance>0</OutputAssemblyInstance><OutputAssemblySize>0</Output
AssemblySize><InputAssemblySize>0</InputAssemblySize><InputAssemblyInstance>0</InputAssemblyInstance></EthernetIpEntity><Pr
ogrammingProtocolEnabled>true</ProgrammingProtocolEnabled><EthernetIpAdapterEnabled>true</EthernetIpAdapterEnabled><ModbusS
erverEnabled>true</ModbusServerEnabled><AutoDiscoveryProtocolEnabled>true</AutoDiscoveryProtocolEnabled></EthernetConfigura
tion><MaxCartridge>1</MaxCartridge><C1TranslationX>170</C1TranslationX><C1TranslationY>110</C1TranslationY><C2TranslationX>
0</C2TranslationX><C2TranslationY>0</C2TranslationY><C1SizeX>155</C1SizeX><C1SizeY>190</C1SizeY><C2SizeX>0</C2SizeX><C2Size
Y>0</C2SizeY><InputAssemblys /><OutputAssemblys /><InputRegisters /><HoldingRegisters /></Cpu><Extensions /><SerialLineConf
iguration><Baud>Baud19200</Baud><ModemReference>No Modem</ModemReference><Parity>ParityEven</Parity><DataBits>DataBits8</Da
taBits><StopBits>StopBits1</StopBits><TimeBetweenFrames>10</TimeBetweenFrames><ResponseTime>10</ResponseTime><StartCharacte
rEnabled>false</StartCharacterEnabled><FirstEndCharacterEnabled>true</FirstEndCharacterEnabled><SecondEndCharacterEnabled>f
alse</SecondEndCharacterEnabled><FrameLengthReceivedAvailable>false</FrameLengthReceivedAvailable><FrameReceivedTimeoutAvai
lable>false</FrameReceivedTimeoutAvailable><InitCommand /><SendFrameCharacter>false</SendFrameCharacter><StartCharacter>0</
StartCharacter><FirstEndCharacter>10</FirstEndCharacter><FrameLengthReceived>0</FrameLengthReceived><FrameReceivedTimeout>0
</FrameReceivedTimeout><SecondEndCharacter>0</SecondEndCharacter><PhysicalMedium>PhysicalMediumRs485</PhysicalMedium><Trans
missionMode>TransmissionModeModbusRtu</TransmissionMode><SlaveId>1</SlaveId><MinTimeBetweenFrames>2</MinTimeBetweenFrames><
Addressing>SlaveAddressing</Addressing><Polarization><Value>0</Value><Name>No</Name></Polarization></SerialLineConfiguratio
n></Plc></HardwareConfiguration><DisplayUserLabelsConfiguration><Languages><UserLabelLanguage><Code>English</Code><Name>Eng
lish</Name></UserLabelLanguage><UserLabelLanguage><Code>French</Code><Name>French</Name></UserLabelLanguage><UserLabelLangu
age><Code>German</Code><Name>German</Name></UserLabelLanguage><UserLabelLanguage><Code>Portuguese</Code><Name>Portuguese</N
ame></UserLabelLanguage><UserLabelLanguage><Code>Spanish</Code><Name>Spanish</Name></UserLabelLanguage><UserLabelLanguage><
Code>Italian</Code><Name>Italian</Name></UserLabelLanguage><UserLabelLanguage><Code>Chinese</Code><Name>Chinese</Name></Use
rLabelLanguage><UserLabelLanguage><Code>Turkish</Code><Name>Turkish</Name></UserLabelLanguage></Languages><Translations /><
/DisplayUserLabelsConfiguration><GlobalProperties><UserInformations /><CompanyInformations /><ProjectInformations><Name>Neu
es Projekt</Name></ProjectInformations><ProjectProtection><Active>true</Active><Password>AAAAAAA</Password><CanView>true</
CanView></ProjectProtection><ApplicationProtection><Active>false</Active></ApplicationProtection><RemoteIpAddresses><IpAddr
esses /></RemoteIpAddresses><ModemConfigurations><ModemConfigurationEntities /></ModemConfigurations><KeepModbusParameters>
false</KeepModbusParameters><UnitId>1</UnitId><DownloadSettings><ResetMemories>true</ResetMemories></DownloadSettings></Glo
balProperties><ReportConfiguration><PageSetup><PaperKind>A4</PaperKind><IsLandscape>false</IsLandscape><ReportUnit>Hundredt
hsOfAnInch</ReportUnit><Top>100</Top><Bottom>100</Bottom><Left>100</Left><Right>100</Right></PageSetup><SubReportConfigurat
ions /></ReportConfiguration></ProjectDescriptor>

>>>
```

[F4] Emacs 78/78 [F3] History [F6] Paste mode
[F2] Menu - CPython 2.7.12

Image 2: Decrypted xml project