Important Security Notification – M340, Quantum. and Premium Ethernet communication modules

May 7, 2013

Schneider Electric® has become aware of multiple vulnerabilities in the Ethernet modules for M340, Quantum, and Premium PLC ranges. This is an update to the document dated Jan 23, 2013.

The vulnerabilities identified include:

(1) For modules that support FTP in the M340 PLC range

> The Ethernet modules crash 50% of the time when using FileZilla as a FTP Client to transfer files to the modules.

(2) For modules that support the Factory Cast feature in the M340, Quantum, Premium PLC ranges

> The FactoryCast service allows the user to send Modbus messages embedded in HTTP POST requests using SOAP.

(3) For modules that support Web Server features in the M340, Quantum, Premium PLC ranges

> The Ethernet module with the Web Server feature allows a user to transmit HTTP commands to the module when the user clicks on maliciously formed hyperlinks. This vulnerability is called Cross Site Request Forgery.

All of these vulnerabilities require network access to the target device.

These vulnerabilities were discovered during cyber security research both by an external researcher and by Schneider Electric internal investigations. We have no evidence that these vulnerabilities have been exploited.

Schneider Electric takes these vulnerabilities very seriously and we have devoted resources to immediately investigate and address these issues. We believe it is critical to consider the whole picture, including safety, security and reliability. Any patches/solutions/mitigations we release will be carefully tested to ensure that they can be deployed in a manner that is both safe and secure.

Details on Products Affected

The following products are vulnerable to an Ethernet module crash when using FileZilla as the FTP Client

<u>M340</u>
The following versions have the fix for this vulnerability:

BMXNOE0100 Firmware version 2.70
BMXNOE0110 Firmware version 5.60
BMXP3420302 Firmware version 2.50
BMXP342020 Firmware version 2.50
BMXP342000 Firmware version 2.50

The following products are vulnerable to receiving Modbus messages embedded in HTTP POST requests using SOAP.

Quantum
140NOE77111
140NWM10000

M340
BMXNOE0110x

Premium
TSXETY5103
TSXWMY100

The following products are vulnerable to a Cross Site Request Forgery vulnerability.

Quantum
140NOE77111
140NOE77101
140NWM10000
140CPU65xxx

M340
BMXNOC0401
BMXNOE0100x
BMXNOE011xx

Premium
TSXETY4103
TSXETY5103
TSXWMY100

The following products support HTTP and FTP service disable feature:

140NOE77101 Firmware Version 06.00

140NOE77111 Firmware Version: 06.00

Details on workarounds and planned fix dates for above described vulnerabilities

1) Ability to crash M340 Ethernet modules when transferring files using FileZilla FTP Client.

Schneider Electric has fixed this issue in the latest released firmware for M340 PLC ranges. Please contact your local Schneider Electric office for latest firmware for M340 PLC range of products. If it is not possible to apply the new firmware to an existing installation at this time, then Schneider Electric has produced a recommendations document that describes firewall and network architecture settings that can be used to mitigate these vulnerabilities. That document is contained in Resolution 207869, Mitigation of vulnerabilities (see link below). Please contact your local Schneider Electric office for more information.

2) Ability to receive Modbus messages via HTTP post using SOAP.

The execution of Modbus messages via SOAP commands is a standard function of the modules that support FactoryCast service. Users have the following options:

(a) If FactoryCast feature is not used but the module is in the network, either

   a. Do not connect this module to un-trusted network

   b. Block all HTTP access using firewall from untrusted network

(b) C. Disable the HTTP service in the module. (Refer to the above list to check if your device is supported)If FactoryCast feature is being used and this module is required to connect to an untrusted network, then use firewall rules that allows HTTP access only from trusted IP Addresses at secured workstations.

Schneider Electric has produced a recommendations document that describes firewall and network architecture settings that can be used to mitigate these vulnerabilities. That document is contained in Resolution 207869, Mitigation of vulnerabilities (see link below). Please contact your local Schneider Electric office for more information.

3) Ability to send commands using Cross Site Request Forgery.

This vulnerability allows the user to send unintentional HTTP commands such as change of the HTTP credentials.

This vulnerability is extremely difficult to exploit as the following conditions have to be met:

- The attacker must determine the URL that would cause a specific outcome
- The attacker must know the right URL inputs
- The attacker must have a way to make the user execute malicious code while authenticated.

To mitigate this vulnerability, the user has the following options:

1) If Web Server feature is not used but have this module is in the network, either

   a. Do not connect this module to untrusted network

   b. Block all HTTP access using firewall from untrusted network

2) Disable the HTTP service in the module. (Refer to the above list to check if your device is supported)If the module is required to connect to untrusted network then use firewall rules that allows HTTP access only from trusted IP Addresses at secured workstations.

Schneider Electric has produced a recommendations document that describes firewall and network architecture settings that can be used to mitigate these vulnerabilities. That document is contained in Resolution 207869, Mitigation of vulnerabilities (see link below). Please contact your local Schneider Electric office for more information.

General Recommendations

Schneider Electric has been designing industrial automation products for many years and recommends to its customers, industry best practices in the development and implementation of control systems. This recommendation includes a Defense in Depth approach to secure an Industrial Control System. This approach places the PLCs behind one or more firewalls to restrict access to authorized personnel and protocols only. The location of the firewalls is decided based on how large the trusted zone is required to be. Please read the following document for more detailed information:

http://download.schneider-electric.com/files?p_File_Id=25779912&p_File_Name=Cyber-Security-STN-v2-Aug-2012.pdf

For Resolution 207869 click link below:
http://download.schneider-electric.com/files?p_File_Id=25575596&p_File_Name=Res207869.pdf

Acknowledgments

Schneider Electric wishes to thank researcher Arthur Gervais for reporting of the vulnerabilities and working with Schneider Electric during the disclosure process

Support CVSS Scoring

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference based on a typical control system, they should be adapted by individual users as required.

(1) Ability to crash M340 PLC range products when transferring files using FileZilla FTP Client: Overall CVSS Score: 4.9 (AV:N/AC:L/Au:S/C:P/I:P/A:P/E:P/RL:O/RC:C/CDP:LM/TD:M/CR:M/IR:M/AR:M)

(2) Ability to do send Modbus messages via HTTP post command: Overall CVSS Score: 2 (AV:N/AC:M/Au:S/C:C/I:C/A:C/E:P/RL:W/RC:UC/CDP:MH/TD:L/CR:M/IR:M/AR:M)

(3) Ability to do Cross Site Request Forgery: Overall CVSS Score: 4.8 (AV:N/AC:M/Au:S/C:P/I:P/A:P/E:P/RL:W/RC:UR/CDP:LM/TD:M/CR:M/IR:M/AR:M)