Important security notification – Quantum and Premium communication modules (ICS-ALERT-12-020-03)

May 7, 2013

Schneider Electric® has become aware of multiple vulnerabilities in the Quantum and Premium Ethernet communication modules. This is an update to the document dated Feb 9, 2012.

The confirmed vulnerabilities identified are:

- HTTP Server Buffer Overflow
- XSS (Cross site scripting) – This vulnerability has only been confirmed to occur on the SNMP configuration web page, which is located in a secure area.
- FTP Server Buffer Overflow – The FTP server has been identified as vulnerable to a buffer overflow. The overflow may occur due on various commands depending on the configuration and firmware version of the module and is not related directly to the CEL command listed at the S4 conference. Modules tested by Schneider did not exhibit this behavior on the listed CEL command but did exhibit this behavior on other messages.

In addition the following vulnerability has been reported but is consistent with current system operation.

- No Authentication between Unity Software and PLC – The Unity to PLC communications for Modbus function code 125 and 126 were not implemented with authentication. The PLC does support a memory protect mode via physical switch that prevent program and configuration changes and a Access Control List to restrict access to the module using Modbus.

The following vulnerability has been reported previously.

- Backdoor accounts – This vulnerability was previously covered in ICSA-12-018-01 (including links to current patches) as well as Schneider Electric resolution RESL206895.

All of these vulnerabilities would 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 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.

Details on Products Affected

The Vulnerabilities are confirmed on the following devices:

- Quantum PLC products: HTTP Server Buffer Overflow, XSS (cross site scripting), FTP Server Buffer Overflow.
- Premium PLC products: FTP Server Buffer Overflow.

The following products are affected:

Quantum (HTTP Buffer Overflow, XSS, FTP Buffer Overflow)

140NOE77101 Firmware Version 4.9 and all previous versions.

140NOE77111 Firmware Version 5.0 and all previous versions.

140NOE77100 Firmware Version 3.4 and all previous versions.

140NOE77110 Firmware Version 3.3 and all previous versions.

140CPU65150 Firmware Version 3.5 and all previous versions.

140CPU65160 Firmware Version 3.5 and all previous versions.

140CPU65260 Firmware Version 3.5 and all previous versions.

Any available Conformal Coated versions of the above part numbers

Premium (FTP Buffer Overflow)

TSXETY4103 Firmware Version 5.0 and all previous versions.

TSXETY5103 Firmware Version 5.0 and all previous versions.

TSXP571634M Firmware Version 4.9 and all previous versions.

TSXP572634M Firmware Version 4.9 and all previous versions.

TSXP573634M Firmware Version 4.9 and all previous versions.

TSXP574634M Firmware Version 3.5 and all previous versions.

TSXP575634M Firmware Version 3.5 and all previous versions.

TSXP576634M Firmware Version 3.5 and all previous versions.

Any available Conformal Coated versions of the above part numbers

The following products support HTTP and FTP service disable feature:

140NOE77101 Firmware Version 06.00

140NOE77111 Firmware Version: 06.00

Recommendations

1) HTTP Server Buffer Overflow.

This vulnerability was remedied in version 5.1 of the 140NOE77101 firmware and Version 3.8 of the 140CPU65150, . 140CPU65160 and 140CPU65260 Ethernet CoPros. Firmware updates are available Schneider-electric.com or on your local country Schneider electric website.

For products awaiting remedies, Schneider Electric recommends limiting access to the HTTP server via external protections such as firewalls.

Schneider Electric has also added a new feature to the models (Refer to list above), which gives user the capability to enable and disable HTTP service in the devices.

For an additional layer of protection against this vulnerability (from internal agents or authorized personnel), a firewall rule set can be found in the following document, Mitigation of Vulnerabilities. Please contact your local representative.

Please note, implementation of this rule **WILL NOT** affect the capacities/functionalities of the product or impact the performance of your installation.

2) XSS (Cross site scripting)

At the present time this vulnerability has only been shown to occur on the SNMP configuration web page which is located in a secure area of the web site, requiring the HTTP password to access.

Schneider Electric recommends disabling this web page by selecting “NO” or “YES” for SNMP configuration instead of “WEB”. This will disable the SNMP configuration web page.

Schneider Electric has added a new feature that allows users to disable HTTP service on modules (Refer to the above list to check if your device is supported)

Please note, implementation of this rule **WILL NOT** affect the capacities/functionalities of the product or impact the performance of your installation but will require the SNMP configuration to be set inside Unity vs on the Web page.

Schneider Electric is investigating a fix for this vulnerability in future product evolutions.

3) FTP Server Buffer Overflow

This vulnerability was remedied in version 5.2 of the TSXETY4103, version 3.8 of the TSXP574634M, TSXP575634M, and TSXP576634M,Ethernet CoPros, and version 5.2 of the Ethernet ports in the TSXP571634M, TSXP572634M and TSXP571634M. Firmware updates are available Schneider-electric.com or by on your local country Schneider electric website.

For products awaiting remedies Schneider Electric recommends limiting access to the FTP service to essential devices to limit exposure to denial of service type attacks. This would include engineering workstations for firmware upgrade/downgrade, and web page updates.

Schneider Electric has also added a new feature to the models (Refer to list above), which gives user the capability to enable and disable FTP service in the devices.

For additional layer of protection against this vulnerability (from internal agents or authorized personnel) a firewall rule set can be found in the following document, Mitigation of Vulnerabilities, please contact your local representative

Please note, implementation of this rule **WILL NOT** affect the capacities/functionalities of the product or impact the performance of your installation.

The current generation of converged Modbus TCP / Ethernet IP modules from Schneider Electric (140NOC77101, TSXETC101) are not vulnerable to this FTP buffer overflow and can be used as a replacement. Schneider Electric recommends checking compatibility before upgrading.

Schneider Electric is expecting to release a fix for the remaining products containing this vulnerability by December 2012.

3a) TFTP Server

The TFTP server is used by the FDR service to allow rapid replacement of field devices. This server allows access to the stored device configuration files only, other areas of the file system cannot be accessed. A denial of service can be generated by filling the file storage area.

Schneider is evaluating options to modify the use of TFTP to preserve the customer experience while improving security, prior to a full resolution the mitigation actions provided in this document will reduce the risk of an exploit of this vulnerability.

4) No Authentication between Unity Software and the PLC

A Modbus tool can be used to send Start and Stop commands to change the state of the PLC. To limit access to these functions Schneider Electric recommends:

a) Implementation of the Access Control List for port 502 (Modbus) on the Messaging tab of the Ethernet communications interface configuration, limiting access to only authorized IP addresses.

b) Limiting access to the module using an external firewall.

c) Setting of the memory protect switch on the PLC to prevent remote modification of the program.

5) General Recommendations

Schneider Electric has been designing industrial automation products for many years; Schneider Electric follows, 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 based on how large the trusted zone is required to be. Please read the following document for more detailed information: **http://www.citect.schneider-electric.com/documents/STN_Ethernet.pdf**

Support

If you are unsure of whether you could be affected by this vulnerability or if you have any questions on this issue please contact your local Schneider Electric support center.