Important Security Notification

Modicon PLC Ethernet Communication Modules

16-Sep-2014

Overview

Schneider Electric® has become aware of a vulnerability in their Ethernet modules for M340, Quantum and Premium PLC ranges as well as other products that provide HTTP services.

Vulnerability Overview

This vulnerability allows an attacker to bypass the basic authentication on the web server. Using directory traversals an attacker can bypass the basic authentication mechanism in the web server and gain unauthorized access to protected resources.

Product(s) Affected

The following part numbers are affected:

140CPU65150	171CCC96020	BMXP3420302H	TSXP572623M	TSXP572634M
140CPU65160	171CCC96020C	BMXP342030H	TSXP572623MC	TSXP573634M
140CPU65260	171CCC96030	BMXPRMxxxx	TSXP572823M	
140NOC77100	171CCC96030C	STBNIC2212	TSXP572823MC	
140NOC78000	171CCC98020	STBNIP2212	TSXP573623AM	
140NOC78100	171CCC98030	TSXETC0101	TSXP573623M	
140NOE77100	BMXNOC0401	TSXETC100	TSXP573623MC	
140NOE77101	BMXNOC0402	TSXETY110WS	TSXP574634M	
140NOE77101C	BMXNOE0100	TSXETY110WSC	TSXP574823AM	
140NOE77110	BMXNOE0110	TSXETY4103	TSXP574823M	
140NOE77111	BMXNOE0110H	TSXETY4103C	TSXP574823MC	
140NOE77111C	BMXNOR0200H	TSXETY5103	TSXP575634M	
140NWM10000	BMXP342020	TSXETY5103C	TSXP576634M	
170ENT11001	BMXP342020H	TSXETZ410	TSXWMY100	
170ENT11002	BMXP342030	TSXETZ510	TSXWMY100C	
170ENT11002C	BMXP3420302	TSXNTP100	TSXP571634M	

Vulnerability Details

This vulnerability allows an attacker to bypass the basic authentication on the web server. Using directory traversals an attacker can bypass the basic authentication mechanism in the web server and gain unauthorized access to protected resources. This vulnerability would require network access to the target device through TCP/IP and particularly HTTP.

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 this issue. 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.

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.

Overall CVSS Score: 9.3
(AV:N/AC:M/Au:N/C:C/I:C/A:C/E:ND/RL:W/RC:C/CDP:H/TD:H/CR:H/IR:H/AR:H)

Mitigation

Schneider Electric has fixed this issue in the latest released firmware for the products listed below:

140CPU65150 Exec v5.5	TSXETY5103 Exec v5.9
140CPU65160 Exec v5.5	TSXETY5103C Exec v5.9
140CPU65260 Exec v5.5	TSXP571634M ETYPort Exec v5.7
140NOC78000 Exec v1.62	TSXP572634M ETYPort Exec v5.7
140NOC78100 Exec v1.62	TSXP573634M ETYPort Exec v5.7
140NOE77101 Exec v6.2	TSXP574634M Ethernet Copro Exec v5.5
140NOE77111 Exec v6.2	TSXP575634M Ethernet Copro Exec v5.5
BMXNOC0401 v2.05	TSXP576634M Ethernet Copro Exec v5.5
BMXNOE0100 v2.9	
BMXNOE0110 Exec v6.0	
BMXNOE0110H Exec v6.0	
TSXETC101 Exec v2.04	
TSXETY4103 Exec V5.7	
TSXETY4103C Exec V5.7	

Latest firmware for the above devices can be found in the following link below, under “Software firmware” -> “Firmware updates”:

http://www.schneider-electric.com/ww/en/download/

Schneider Electric recommends the following measures to mitigate the vulnerability for the remaining affected devices:

- Use a deep packet inspection firewall to prevent HTTP requests to the product that contain traversals in the URL.
- Disable port 80 (HTTP) on modules where it is possible
- Block port 80 in firewalls to these devices, except for trusted devices.

Please contact Schneider Electric Customer Care Center for more information.

For More Information

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 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_Reference=STN v2&p_EnDocType=Technical leaflet&p_File_Id=305147922&p_File_Name=Cyber+Security+STN+v2+Aug-2012.pdf

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric’s products, please visit Schneider Electric’s cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com