Important Security Notification

Modicon PLC Web Servers

September 3, 2015

Overview

Schneider Electric has become aware of a vulnerability in the web servers deployed in the Modicon PLC product line.

This vulnerability is also covered in ICS-ALERT-15-224-02

Vulnerability Overview

The vulnerability identified allows Remote File Inclusion (client side execution of java script) and Reflected XSS (non-persistent) through the use of specially crafted URLs.

In addition the public release of this vulnerability notes a previous vulnerability related to hard coded credentials on the FTP server. The FTP server can be disabled by following the instructions in this resolution document:

http://www.schneider-electric.com/ww/en/download/document/Res206895

Product(s) Effected

The products listed :

- BMXNOC0401
- BMXNOE0100
- BMXNOE0110
- BMXNOE0110H
- BMXNOR0200H
- BMXP342020
- BMXP342020H
- BMXP342030
- BMXP3420302
- BMXP3420302H
- BMXP342030H

All firmware versions and conformally coated versions of the above products are effected.

In addition Schneider Electric is investigating this issue on other products and will update this document as more information becomes available.

Vulnerability Details

- Remote File Inclusion allows an attacker to craft a specific URL referencing the PLC web server which, when launched, will result in the browser redirecting to a remote file via a java script loaded with the web page.

- Reflected Cross Site Scripting (non persistent) allows an attacker to craft a specific URL which contains Java script that will be executed on the client browser.

- In both of the above vulnerabilities the attacker must, by social engineering or other means, cause a person with HTTP access to the PLC Web server to click on the specifically crafted web link. In addition, the attacker must know the IP address of the target PLC in order to craft the link.

Schneider Electric would like to thank J. Francisco Bolivar and Aditya K. Sood for their support in identifying these vulnerabilities.

Mitigation

To address this vulnerability, Schneider Electric will release a firmware patch for the listed products by August 31,’ 2015. It will initially only be available through Schneider Electric’s Customer Support teams, and then included in the next scheduled product firmware update.

BMX NOE 0100	v3.00 IR32
	Web v4.50 IR10
BMX NOE 0110	v6.10 IR04
	Web v6.10 IR05
BMX NOC 0401	v2.06 IR01
	Web v1.30 IR03
M340 P34 xxxx	v4.60 IR02
	Web v4.60 IR02

After updating the module firmware it is recommended that the PC Web Cache be deleted.

In addition, specific modules and firmware versions allow the HTTP/FTP server to be disabled through configuration settings, please consult your product documentation for further information.

For other modules and firmware, Schneider Electric has produced a recommendations document that describes firewall and network architecture settings that can be used to mitigate these types of vulnerabilities (Resolution 207869, Mitigation of Vulnerabilities).

http://www.schneider-electric.com/ww/en/download/document/Res207869

For More Information

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 cyber security web page: 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

Revision Control:

Version A	Pg. 1 - Remove BMXNOC0402 part number from impacted product list Pg. 2 – add specific versions of patched firmware
Version B	Pg. 2 – Add sentence regarding deleting of cache

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2016.02.10 14:06:28 -05'00'