GoAhead Web Server vulnerability

December 10th, 2015

Overview

Schneider Electric has become aware of a vulnerability in the Modicon M340 product line.

Vulnerability Overview

A vulnerability has been identified, in Schneider Electric Industrial Ethernet devices that allows an attacker to cause a buffer overflow situation using the web server login mechanism to halt operation of the device or remotely execute code.

A CVSS base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).

Product(s) Affected

The product(s) or product lines affected include:

- BMXNOC0401 (all versions prior to v2.09)
- BMXNOE0100 (all versions prior to v3.10)
- BMXNOE0100H (all versions prior to v3.10)
- BMXNOE0110 (all versions prior to v6.30)
- BMXNOE0110H (all versions prior to v6.30)
- BMXNOR0200 (all versions prior to v1.70)
- BMXNOR0200H (all versions prior to v1.70)
- BMXP342020 (all versions prior to v2.80)
- BMXP342020H (all versions prior to v2.80)
- BMXP342030 (all versions prior to v2.80)
- BMXP3420302 (all versions prior to v2.80)
- BMXP3420302H (all versions prior to v2.80)
- BMXPRA0100 (all versions prior to v2.80)

Vulnerability Details

Attack steps:

1. The attacker identifies a protected URL that they wish to attack. This can be done either by reverse engineering a purchased product, by gathering information in HTTP queries to the product, or from disclosed information from the Internet.

   For example, the attacker may identify the URL of the global data page:

   http://[HostName]/secure/system/globaldata.htm

2. Since this page is part of the 'secure' directory, User name and Password entry fields pop up to protect the resource:

3. The attacker enters a password greater than 65 characters into the Password field (Generally between 90-100 characters is enough to cause the device to crash) and presses OK (no username is required).

4. The web server handles the request and attempts to copy the oversized password into a 65-character buffer using **`strcpy()`**, which is void of buffer length protection.

Effects:

- The device the attacker is accessing crashes.
- It may be possible to construct a password to pass to the server that could remotely execute code in memory on the device. (This has not been verified.)

Schneider Electric would like to thank CyberX for their support in identifying this vulnerabilities.

Mitigation

Possible workaround:

- Block port 80 using a firewall.

Possible fixes and Plan Fix Date

- New firmware will be developed and release for the modules affected

Firmware	Release dates
BMXNOC0401	Dec-15
BMXNOE0100 (H)	Dec-15
BMXNOE0110 (H)	Dec-15
BMXNOR0200 (H)	Jan-16
BMXP342020	Jan-16
BMXP3420302	Jan-16
BMXPRA0100	Jan-16

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 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

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Strategy & Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2015.12.15 13:44:51 -05'00'