Schneider Electric Security Notification

GoAhead Web Server vulnerability (V2.0)

10 December 2015 (9 June 2020)

Overview

Schneider Electric is aware of a proof of concept exploit available for this vulnerability. It is imperative that customers upgrade the firmware for the affected products.

Affected Product(s)

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

CVE ID: **CVE-2015-7937**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Stack-based buffer overflow in the GoAhead Web Server on Schneider Electric Modicon M340 PLC BMXNOx and BMXPx devices allows remote attackers to execute arbitrary code.

Remediation

Refer to latest firmware version listed below for fixed versions of the affected products:

Affected Product	Remediation
BMXNOC0401	https://www.se.com/ww/en/product/BMXNOC0401/ethernet-module-m340---4-x-rj45-10-100/#pdp-software
BMXNOE0100	https://www.se.com/ww/en/product/BMXNOE0100/ethernet-module-m340---flash-memory-card---1-x-rj45-10-100/#pdp-software
BMXNOE0100H	https://www.se.com/ww/en/product/BMXNOE0100/ethernet-module-m340---flash-memory-card---1-x-rj45-10-100/#pdp-software
BMXNOE0110	https://www.se.com/ww/en/product/BMXNOE0110/ethernet-module-m340---flash-memory-card---internal-ram-16-mb---1-x-rj45-10-100/#pdp-software
BMXNOE0110H	https://www.se.com/ww/en/product/BMXNOE0110/ethernet-module-m340---flash-memory-card---internal-ram-16-mb---1-x-rj45-10-100/#pdp-software
BMXNOR0200	https://www.se.com/ww/en/product/BMXNOR0200H/ethernet---serial-rtu-module---2-x-rj45/#pdp-software
BMXNOR0200H	https://www.se.com/ww/en/product/BMXNOR0200H/ethernet---serial-rtu-module---2-x-rj45/#pdp-software
BMXP342020	https://www.se.com/us/en/product/BMXP342020/processor-module-m340%2C-max-1024-discrete-and-256-analog-i-o%2C-modbus%2C-ethernet/#pdp-software
BMXP342020H	https://www.se.com/us/en/product/BMXP342020/processor-module-m340%2C-max-1024-discrete-and-256-analog-i-o%2C-modbus%2C-ethernet/#pdp-software
BMXP342030	This model has reached its end of life inn 2009. Please apply the mitigations below. Contact your local technical support for more information.
BMXP3420302	https://www.se.com/us/en/product/BMXP3420302/processor-module-m340---max-1024-discrete-%2B-256-analog-i-o---canopen/#pdp-software

BMXP3420302H	https://www.se.com/us/en/product/BMXP3420302/processor-module-m340---max-1024-discrete-%2B-256-analog-i-o---canopen/#pdp-software
BMXPRA0100	https://www.se.com/au/en/product/BMXPRA0100/modicon-x80-peripheral-remote-io-adaptor-module/#pdp-software

Customers are advised that the webserver is disabled by default. Because web services are only necessary for specific maintenance, configuration, or monitoring activities, it is advised to disable web services all together during times when the services are not needed. Customers are also advised to:

- Configure access control lists to restrict web server access to authorized IP addresses.
- Protect access to Modicon products with network, industrial, and application firewalls.

Product Information

GoAhead Web Server is the webserver component used on Schneider Electric Modicon M340 PLC BMXNOx and BMXPx devices.

Product Category - All Categories

Learn more about Schneider Electric's product categories here: https://www.se.com/us/en/all-products

How to determine if you are affected

Products affected are listed in "Affected products" above with webserver service activated.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Never connect programming software to any network other than the network for the devices that it is intended.

- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow laptops that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems, and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2015-7937	CyberX

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN “AS-IS” BASIS WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO

IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and digital automation** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *10 December 2015*	Original Release
Version 2 *9 June 2020*	Updated overview and remediation section (pages 1-3)

Product Security Office

Digitally signed by Product Security Office
Date: 2020.06.07 12:37:31 -04'00'