Schneider Electric Security Notification

Modicon Ethernet / Serial RTU Module

13 August 2019

Overview

Schneider Electric is aware of multiple vulnerabilities in the BMXNOR0200H Ethernet / Serial RTU module products.

Affected Product(s)

BMXNOR0200H Ethernet / Serial RTU module - all firmware versions

Vulnerability Details

CVE ID: **CVE-2019-6813**

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

A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists which could cause denial of service when truncated SNMP packets on port 161/UDP are received by the device.

Customers are strongly encouraged to apply the following mitigation to reduce risk:

- Setup network segmentation and implement a firewall to block all unauthorized access to SNMP port 161/UDP.

CVE ID: **CVE-2019-6831**

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

A CWE-754: Improper Check for Unusual or Exceptional Conditions vulnerability exists which could cause disconnection of active connections when an unusually high number of IEC 60870-5-104 packets are received by the module on port 2404/TCP.

Customers are strongly encouraged to apply the following mitigation to reduce risk:

- Setup network segmentation and implement a firewall to block all unauthorized access to port 2404/TCP.

Schneider Electric Security Notification

CVE ID: **CVE-2019-6810**

CVSS v3.0 Base Score 8.6 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H

A CWE-284: Improper Access Control vulnerability exists which could cause the execution of commands by unauthorized users when using IEC 60870-5-104 protocol.

Customers are strongly encouraged to apply the following mitigation to reduce risk:

- Setup network segmentation and implement a firewall to block all unauthorized access to port 2404/TCP.

Product Information

The BMXNOR0200H Ethernet / Serial RTU module is part of the Modicon X80 I/O product category. Modicon X80 I/Os are common platform of modules for Modicon M580 and M340 PLCs

Product Category - All Categories

Learn more about Schneider Electric's product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected

BMXNOR0200H Ethernet / Serial RTU module connected to an Ethernet network

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the "Program" mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or 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), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is 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-2019-6810, CVE-2019-6813, CVE-2019-6831	VAPT Team (C3i IITK, UP, India)

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

About Schneider Electric

Schneider Electric Security Notification

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

We provide **energy and automation digital** 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 with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *13 August 2019*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2019.08.12 11:34:30 -04'00'