Schneider Electric Security Notification

OPC UA and X80 Advanced RTU
Modicon Communication Modules

12 July 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in its BMENUA0100 - OPC UA module and BMENOR2200H X80 advanced RTU communication module for M580.

The BMENUA0100 - OPC UA module for M580 is an Ethernet communications module with an embedded OPC UA server for communication with OPC UA clients, including SCADA.

The BMENOR2200H – X80 advanced RTU module is an Ethernet communication module that enables M580 platform to use RTU protocol exchange with RTU stations.

Failure to apply the mitigations provided below may introduce risks including denial of service of the webserver and bypass of the secure boot process, which could result in running an unauthorized firmware.

Affected Products and Versions

Affected Products and Versions	CVE-						
	2022-34759	2022-34760	2022-34761	2022-34762	2022-34763	2022-34764	2022-34765
OPC UA Modicon Communication Module (BMENUA0100) *V1.10 and prior*	X	X	X	X	X	X	X
X80 advanced RTU Communication Module (BMENOR2200H) *V1.0*	X	X				X	
X80 advanced RTU Communication Module (BMENOR2200H) *V2.01 and later*			X	X	X		X

Vulnerability Details

CVE ID: **CVE-2022-34759**

CVSS v3.1 Base Score 7.5 | High | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A *CWE-787: Out-of-bounds Write* vulnerability exists that could cause a denial of service of the webserver due to improper parsing of the HTTP Headers.

Schneider Electric Security Notification

CVE ID: **CVE-2022-34760**

CVSS v3.1 Base Score 7.5 | High | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A *CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop')* vulnerability exists that could cause a denial of service of the webserver due to improper handling of the cookies.

CVE ID: **CVE-2022-34761**

CVSS v3.1 Base Score 7.5 | High | AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A *CWE-476: NULL Pointer Dereference* vulnerability exists that could cause a denial of service of the webserver when parsing JSON content type.

CVE ID: **CVE-2022-34762**

CVSS v3.1 Base Score 5.9 | Medium | AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')* vulnerability exists that could cause unauthorized firmware image loading when unsigned images are added to the firmware image path.

CVE ID: **CVE-2022-34763**

CVSS v3.1 Base Score 5.9 | Medium | AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:H/A:H

A *CWE-345: Insufficient Verification of Data Authenticity* vulnerability exists that could cause loading of unauthorized firmware images due to improper verification of the firmware signature.

CVE ID: **CVE-2022-34764**

CVSS v3.1 Base Score 5.9 | Medium | AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

A *CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer* vulnerability exists that could cause denial of service when parsing the URL.

CVE ID: **CVE-2022-34765**

CVSS v3.1 Base Score 5.5 | Medium | AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H

A *CWE-73: External Control of File Name or Path* vulnerability exists that could cause loading of unauthorized firmware images when user-controlled data is written to the file path.

Schneider Electric Security Notification

Remediations & Mitigations

Affected Product & Version	Mitigations
OPC UA Modicon Communication Module (BMENUA0100) *V1.10 and prior*	Schneider Electric is establishing a remediation plan for all future versions of OPC UA Modicon Communication Module BMENUA0100 that will include a fix for these vulnerabilities. We will update this document when the remediation is available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit: • Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP • Configure BMENUA0100 module to operate in Secured mode. Refer to the user manual below in the section 'Cybersecurity Operating Modes' and change the default passwords. • Configure role-based access control and local authentication for users of BMENUA0100 module. Refer to the 'Access Control' section in the user manual • User Manual: https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=PHA83350.03.pdf&p_Doc_Ref=PHA83350 • Use IPSEC to help secure Ethernet communication. • Download the firmware updates from the Schneider Electric website and verify the firmware integrity To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp
X80 advanced RTU Communication Module (BMENOR2200H) All versions	BMENOR2200H V2.01 and later include a fix for CVE-2022-34759, CVE-2022-34760, and CVE-2022-34764. The latest firmware version is available for download here: https://www.se.com/ww/en/product/BMENOR2200H/x80-advanced-rtu-module-ethernet-based-1-serial-port-hardened/ Vulnerabilities CVE-2022-34762, CVE-2022-34765, CVE-2022-34763, and CVE-2022-34761 have been introduced since V2.01. Schneider Electric is establishing a remediation plan for all future versions of X80 advanced RTU Communication Module BMENOR2200H that will include a fix for these vulnerabilities. We will update this document when the remediation is available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit:

	• Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP • Configure BMENOR2200H module to operate in Secured mode. Refer to the user manual below in the section 'Cyber Security Configuration' and change the default passwords. • Configure role-based access control and local authentication for users of BMENOR2200H module. Refer to the 'RBAC' section in the user manual • User Manual: https://download.schneider-electric.com/files?p_Doc_Ref=PHA90072&p_enDocType=User+guide&p_File_Name=PHA90072.02.pdf • Use IPSEC to help secure Ethernet communication. • Download the firmware updates from the Schneider Electric website and verify the firmware integrity To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp

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 intended for that device.
- 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 mobile devices 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.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

Schneider Electric Security Notification

Acknowledgements

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researchers
CVE-2022-34759, CVE-2022-34760, CVE-2022-34761, CVE-2022-34762, CVE-2022-34763, CVE-2022-34764, CVE-2022-34765	Ryan Hall and Vlad Ionescu, Meta Red Team X

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, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

About Schneider Electric

Schneider's purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

Schneider Electric Security Notification

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.
www.se.com

Revision Control:

Version 1.0 *12 July 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.07.11 14:23:02 -04'00'