Schneider Electric Security Notification

Web Server on Modicon M340, Modicon Quantum and Modicon Premium Legacy offers and their Communication Modules

13 October 2020

Overview

Schneider Electric is aware of a vulnerability in the web server of the Modicon M340, Modicon Quantum and Modicon Premium Legacy offers and their communication modules.

The Modicon Ethernet Programmable Automation products are controllers for industrial process and infrastructure.

Failure to apply the remediations provided below may risk execution of commands on the webserver by an authenticated attacker, which could result in loss of availability, confidentiality and integrity on the controller.

Affected Products and Versions

- **M340 CPUs**
  - BMX P34x prior to firmware version 3.20
- **M340 Communication Ethernet modules**
  - BMX NOE 0100 (H) prior to version 3.3
  - BMX NOE 0110 (H) prior to version 6.5
  - BMX NOC 0401 prior to version 2.10
- **Premium processors with integrated Ethernet COPRO**
  - TSXP574634, TSXP575634, TSXP576634 prior to 6.1 version
- **Premium communication modules**
  - TSXETY4103 prior to version 6.2
  - TSXETY5103 prior to version 6.4
- **Quantum processors with integrated Ethernet COPRO**
  - 140CPU65xxxxx prior to 6.1 version
- **Quantum communication modules**
  - 140NOE771x1 prior to version 7.1
  - 140NOC78x00 prior to version 1.74
  - 140NOC77101 prior to version 1.08

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2020-7533**

CVSS v3.0 Base Score 10.0 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

A CWE-255: Credentials Management vulnerability exists which could cause the execution of commands on the webserver without authentication when sending specially crafted HTTP requests.

Remediation

These vulnerabilities are fixed and available for download in in the firmware versions listed below.

M340 version 3.20 firmware	
BMXP3420302 and CL and H	https://www.se.com/en/download/document/BMXP3420302_Firmwares/
BMXP342020 and H	https://www.se.com/en/download/document/BMXP342020_Firmwares/
BMXP342000	https://www.se.com/en/download/document/BMXP342000_Firmwares/
BMXP341000 and H	https://www.se.com/en/download/document/BMXP341000_Firmwares/
BMXP3420102 and CL	https://www.se.com/en/download/document/BMXP3420102_Firmwares/
BMXP3420302	https://www.se.com/en/download/document/BMXP3420302_Firmwares

M340 Communication Ethernet modules	
BMXNOE0100 and H version 3.3	https://www.se.com/ww/en/download/document/BMXNOE0100%20Exec%20and%20Release%20Notes/
BMXNOE0110 and H version 6.5	https://www.se.com/ww/en/download/document/BMXNOE0110%20Exec%20and%20Release%20Notes/
BMXNOC0401 version 2.10	https://www.se.com/ww/en/download/document/BMXNOC0401%20Exec%20and%20Release%20Notes/

Premium Offers	
Premium processors with integrated Ethernet COPRO version 6.1 - product references TSXP574634, TSXP575634, TSXP576634	https://www.se.com/ww/en/download/document/TSXP574634M%20Premium%20Copro%20Exec%20and%20Release%20Notes/
TSXETY4103 version 6.2	https://www.se.com/ww/en/download/document/TSXETY4103%20Exec%20and%20Release%20Notes/
TSXETY5103 version 6.4	https://www.se.com/ww/en/download/document/TSXETY5103%20Exec/

Quantum Offers	
Quantum processors with integrated Ethernet COPRO version 6.1 – product reference 140CPU65xxxxx	https://www.se.com/ww/en/download/document/140CPU65260%20Quantum%20Copro%20Exec%20and%20Release%20Notes/
140NOE771x1 version 7.1	https://www.se.com/ww/en/download/document/140NOE77111%20Exec%20and%20Release%20Notes%20For%20Unity%20and%20Non%20Unity%20Users/
140NOC78x00 version 1.74	https://www.se.com/ww/en/download/document/140NOC78000%20Exec%20and%20Release%20Notes/
140NOC77101 version 1.08	https://www.se.com/ww/en/download/document/140NOC77101%20Exec%20and%20Release%20Notes/

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

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 for.
- 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.

Acknowledgements

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

CVE	Researcher Name
CVE-2020-7533	Yang Dong (DingXiang Dongjian Security Lab)

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 or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Schneider Electric Security Notification

SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, 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. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. 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 **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 October 2020*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2020.10.11 17:01:53 -04'00'