Schneider Electric Security Notification

Security Notification – Embedded Web Servers for Modicon (V3.2)

23 November 2018 (12 May 2020)

Overview

Schneider Electric is aware of multiple vulnerabilities in the HTTP (web) server of its Modicon family of programmable logic controllers. Users are advised to take the necessary steps to secure their PLCs.

Failure to address these vulnerabilities could result in unauthorized access to the controllers, denial of service and/or other malicious activity.

Affected Product(s)

The products affected include all Modicon M340, Premium, Quantum PLCs and BMXNOR0200 controllers.

Vulnerability Details

CVE ID: CVE-2018-7811

CVSS v3.0 Base Score 9.8 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A CWE-620: Unverified Password Change vulnerability exists on the embedded web server which could allow an unauthenticated remote user to access the “change password” function of the web server.

CVE ID: CVE-2018-7809

CVSS v3.0 Base Score 6.5 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L

A CWE-620: Unverified Password Change vulnerability exists, which could allow an unauthenticated remote user to access the “password delete” function of the web server.

CVE ID: CVE-2018-7810

CVSS v3.0 Base Score 6.1 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

A CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability exists, which could allow an attacker to craft a URL containing

JavaScript that would be executed within the user's browser, potentially impacting the machine the browser is running on.

CVE ID: CVE-2018-7831

CVSS v3.0 Base Score 8.8 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A CWE-352: Cross-Site Request Forgery (CSRF) vulnerability exists, which could allow an attacker to send a specially crafted URL to a currently authenticated web server user to execute a password change on the web server.

CVE ID: CVE-2018-7830

CVSS v3.0 Base Score 5.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

A CWE-113: Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') vulnerability exists, where a denial of service can occur for ~1 minute by sending a specially crafted HTTP request.

CVE ID: CVE-2018-7804

CVSS v3.0 Base Score 4.7 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:L

A CWE-601: URL Redirection to Untrusted Site vulnerability exists, where a user clicking on a specially crafted link can be redirected to a URL of the attacker's choosing.

CVE ID: CVE-2018-7812

CVSS v3.0 Base Score 5.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

A CWE-203: Information Exposure Through Discrepancy vulnerability exists, where the web server sends different responses in a way that exposes security-relevant information about the state of the product, such as whether a particular operation was successful or not.

CVE ID: CVE-2018-7833

CVSS v3.0 Base Score 7.5 | (Medium) | CVSS:3.0/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, where an unauthenticated user can send a specially crafted XML data via a POST request to cause the web server to become unavailable.

Remediation

Schneider Electric recommends customers follow the instructions outlined in the Modicon Controllers Platform Cyber Security Reference Manual to install Modicon PLCs securely.

Schneider Electric Security Notification

Customers are advised that the web server 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.

Fixes for **CVE-2018-7833** and **CVE-2018-7804**

- The vulnerabilities are fixed for M340 controller in the version V3.20. The fix is available for download below:

M340 V3.20 firmware	
BMXP3420302 and CL and H	https://www.schneider-electric.com/en/download/document/BMXP3420302_Firmwares/
BMXP342020 and H	https://www.schneider-electric.com/en/download/document/BMXP342020_Firmwares/
BMXP342000	https://www.schneider-electric.com/en/download/document/BMXP342000_Firmwares/
BMXP341000 and H	https://www.schneider-electric.com/en/download/document/BMXP341000_Firmwares/
BMXP3420102 and CL	https://www.schneider-electric.com/en/download/document/BMXP3420102_Firmwares/

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.
- 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 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 would like to recognize the following researcher(s) for all their efforts related to identification and coordination of this vulnerability:

CVE	Researcher(s) Name
CVE-2018-7809, CVE-2018-7810, CVE-2018-7830, CVE-2018-7831	Tenable, Inc.
CVE-2018-7811	Tenable, Inc. and VAPT Team/C3i Center (IIT Kanpur, India)
CVE-2018-7812	David Castro, Head of Red Team at Novared Spain
CVE-2018-7804	Ismail Tasdelen
CVE-2018-7833	Qingtang Zheng (CodeSafe Team of Legendsec at Qi'anxin Group)

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

Schneider Electric Security Notification

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 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 about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *23-Nov-2018*	Original Release
Version 1.1 *28-Nov-2018*	CVSS Scores updated for CVE-2018-7811 (page 1) and CVE-2018-7810 (page 2)
Version 2 *13-Dec-2018*	Added CVE-2018-7804, CVE-2018-7812, CVE-2018-7833 (page 2 and 3)
Version 2.1 *09-May-2019*	Added researcher to acknowledgement section for CVE-2018-7811(page 4)
Version 2.2 *11-Jun-2019*	CVE-2018-7833 researcher acknowledgment updated (page 4)
Version 3.0 *08-Oct-2019*	CVE-2018-7833 - Fix available for M340 controller CVE-2018-7804 - Fix available for M340 controller (page 3)
Version 3.1 *27-Nov-2019*	CVE-2018-7831 – Corrected CWE ID and CVSS score (page 3)
Version 3.2 *12-May-2020*	Corrected CVSS vector for CVE-2018-7812 (page 2)

Product Security Office

Digitally signed by Product Security Office
Date: 2020.05.11 13:33:48 -04'00'