Schneider Electric Security Notification

Security Notification – Embedded Web Servers for Modicon V2

23 November 2018 **(Updated 11 Jun 2019)**

Overview

Schneider Electric has been made aware of multiple vulnerabilities in the HTTP (web) server of its Modicon PLC family of products are advised to take the necessary steps to secure their Modicon PLC(s). Failure to address these vulnerabilities could result in unauthorized access to the PLC(s), denial of service, and/or other malicious activity.

Affected Product(s)

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

Vulnerability Details

CVE ID: CVE-2018-7811

CVSS: 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: 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: 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 allowing an attacker to craft a URL containing JavaScript that will be executed within the user's browser, potentially impacting the machine the browser is running on.

Schneider Electric Security Notification

CVE ID: CVE-2018-7831

CVSS: 5.4 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L

A CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability exists allowing 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: 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: 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: 5.3 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/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: 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.

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

General Security Recommendations

The following industry cybersecurity best practices are strongly advised:

- 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.

Schneider Electric Security Notification

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 is intended to help provide an overview of the identified situation and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

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

If you require additional support, Schneider Electric Industrial Cybersecurity Services team are available to help. Please visit: https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Schneider Electric Security Notification

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.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)

Product Security Office

Digitally signed by Product Security Office
Date: 2019.06.10 09:29:23 -04'00'