Security Notification – Embedded Web Servers for Modicon

22-Mar-2018

Overview

Schneider Electric has become aware of multiple vulnerabilities in the HTTP (web) servers of its Modicon PLC family of products, as reported by the cybersecurity research firm Positive Technologies. Please take the necessary steps now to secure your Modicon PLC. Failure to address these vulnerabilities could result in unauthorized access to your PLC and a denial of service or other malicious activity.

Vulnerability Overview

The reported vulnerabilities could enable unauthorized access, arbitrary code execution, or denial of service on the Modicon PLCs.

Product(s) Affected

The product(s) affected include all Modicon M340, Premium, Quantum PLCs and BMXNOR0200.

Mitigation

Schneider Electric recommends customers follow the instructions outlined in the *Modicon Controllers Platform Cyber Security Reference Manual* to install your Modicon PLCs securely. We also recommend:

- Properly configure the access control list in order to restrict access to web server only to authorized IP addresses
- Protect access to your Modicon products via a firewall
- Web server is disabled by default. Because web services are only necessary for specific maintenance, configuration or monitoring activities, we advise to disable web services altogether during times when the service is not needed

For customers requiring additional support, Schneider Electric's Industrial Cybersecurity Services team are available to help with assessments and deployment support. Please visit us for more information: https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Vulnerability Details

CVE	Vulnerability	Detailed description	CVSS Base score	Impacted products
CVE-2018-7759	Denial of service due to bad management of SOAP requests length	Buffer overflow is caused by the length of the source string specified (instead of the buffer size) as the number of bytes to be copied	5.9 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	All versions of FactoryCast products (Modicon Premium, Quantum, M340)
CVE-2018-7760	Authorization bypass on CGI requests	Requests to CGI functions allow malicious users to bypass authorization	7.7 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L	All versions of embedded web servers in Modicon Premium, Quantum, M340 and BMXNOR0200
CVE-2018-7761	Arbitrary code execution	Vulnerability in HTTP request parser	7.3 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L	BMXNOR 0200 all versions
CVE-2018-7762	Buffer overflow	Vulnerability in web services to process SOAP requests	5.9 CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H	All versions of FactoryCast products (Modicon Premium, Quantum, M340)

Acknowledgements

Schneider Electric would like to thank the following for helping to identify these vulnerabilities:

CVE-2018-7759

- Nikita Maximov (Positive Technologies)

CVE-2018-7760

- Alexey Stennikov (Positive Technologies)
- Anton Dorfman (Positive Technologies)

CVE-2018-7761

- Alexander Melkikh (Positive Technologies)
- Yuliya Simonova (Positive Technologies)

CVE-2018-7762

- Nikita Maximov (Positive Technologies)

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

About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

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 *22 March 2018*	Original Release

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2018.03.22 17:24:50 -04'00'