Schneider Electric Security Notification

Security Notification – IIoT Monitor

20 December 2018 (14 January 2019)

Overview

Schneider Electric has become aware of multiple vulnerabilities in the IIoT Monitor product.

Affected Product(s)

IIoT Monitor 3.1.38

Vulnerability Details

CVE ID: CVE-2018-7835

CVSS: 7.5 | (High) | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists which could allow access to files available to SYSTEM user.

CVE ID: CVE-2018-7836

CVSS: 9.3 | (Critical) | AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N

A CWE-434: Unrestricted Upload of File with Dangerous Type vulnerability exists on numerous methods of the IIoT Monitor software that could allow upload and execution of malicious files.

CVE ID: CVE-2018-7837

CVSS: 7.5 | (High) | AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A CWE-611: Improper Restriction of XML External Entity Reference ('XXE') vulnerability exists on numerous methods of the IIoT Monitor software that could allow the software to resolve documents outside of the intended sphere of control, causing the software to embed incorrect documents into its output and expose restricted information.

CVE ID: CVE-2018-7839

CVSS: 6.5 | (Medium) | AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

A CWE-310: Cryptographic Issue vulnerability exists which could allow information disclosure.

Remediation

Users of IIoT Monitor Software are advised to contact Schneider Electric customer support for assistance in migrating to the latest software solution that resolves these vulnerabilities.

https://www.schneider-electric.com/en/work/support/contacts.jsp

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.
- 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.

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-2018-7835, CVE-2018-7836, CVE-2018-7837, CVE-2018-7839	Rgod via ZDI (Zero Day Initiative)

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

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND MITIGATION ACTIONS, AND IS PROVIDED ON AN "AS-IS" BASIS AND IS NOT INTENDED AS A WARRANTY OR GUARANTEE OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. 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

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 *20 December 2018*	Original Release
Version 1.1 *14 January 2019*	Page 2 – Added CVE-2018-7839

Product Security Office

Digitally signed by Product Security Office
Date: 2019.01.14 16:29:11 -05'00'