Security Notification – U.motion Builder

31-May-2018

Overview

Schneider Electric has become aware of multiple vulnerabilities in the U.motion Builder product.

Vulnerability Overview

The vulnerabilities identified are:

- CVE-2018-7784 - Print Format Vulnerability
- CVE-2018-7785 - Remote Command Injection
- CVE-2018-7786 - Cross Site Scripting
- CVE-2018-7787 - Improper Input Validation

Product(s) Affected

The product(s) affected:

- U.motion Builder, all versions prior to 1.3.4

Vulnerability Details

CVE ID: CVE-2018-7784

This exploit occurs when the submitted data of an input string is evaluated as a command by the application. In this way, the attacker could execute code, read the stack, or cause a segmentation fault in the running application.

Overall CVSS Score: 10.0 (Critical)

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE ID: CVE-2018-7785

A remote command injection allows authentication bypass

Overall CVSS Score: 10.0 (Critical)

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVE ID: CVE-2018-7786

A cross site scripting (XSS) vulnerability exists which could allow injection of malicious scripts.

Overall CVSS Score: 6.1 (Medium)

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVE ID: CVE-2018-7787

This vulnerability is due to improper validation of input of context parameter in HTTP GET request

Overall CVSS Score: 5.3 (Medium)

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Mitigation

A fix for this vulnerability is available for download below, version 1.3.4:

https://www.schneider-electric.com/en/download/document/Umotion_Server_update/

Acknowledgements

bigric3@360A-TEAM

- CVE-2018-7784
- CVE-2018-7785
- CVE-2018-7786

Wei Gao (Ixia A Keysight Business)

- CVE-2018-7787

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 *31 May 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: 2018.06.01 14:24:44 -04'00'