Schneider Electric Security Notification

U.motion Server

10 September 2019

Overview

Schneider Electric is aware of multiple vulnerabilities in its U.motion din rail and touch panel servers.

Affected Product(s)

U.motion servers:

- MEG6501-0001 - U.motion KNX server
- MEG6501-0002 - U.motion KNX Server Plus
- MEG6260-0410 - U.motion KNX Server Plus, Touch 10
- MEG6260-0415 - U.motion KNX Server Plus, Touch 15

Vulnerability Details

CVE ID: **CVE-2019-6835**

CVSS v3.0 Base Score 5.4 | (Medium) | CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

A Cross-Site Scripting (XSS) CWE-79 vulnerability exists, which could allow an attacker to inject client-side script when a user visits a web page.

CVE ID: **CVE-2019-6836**

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

An Improper Access Control: CWE-284 vulnerability exists, which could allow the file system to access the wrong file.

CVE ID: **CVE-2019-6837**

CVSS v3.0 Base Score 9.6 | (Critical) | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N

A Server-Side Request Forgery (SSRF): CWE-918 vulnerability exists, which could cause server configuration data to be exposed when an attacker modifies a URL.

CVE ID: **CVE-2019-6838**

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

An Improper Access Control: CWE-284 vulnerability exists, which could allow a user with low privileges to delete a critical file.

CVE ID: **CVE-2019-6839**

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

An Improper Access Control: CWE-284 vulnerability exists, which could allow a user with low privileges to upload a rogue file.

CVE ID: **CVE-2019-6840**

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 Format String: CWE-134 vulnerability exists, which could allow an attacker to send a crafted message to the target server, thereby causing arbitrary commands to be executed.

Remediation

The vulnerabilities are fixed in version 1.3.7 and is available for download below:

U.motion Server Part Number	Download Link
MEG6501-0001 - U.motion KNX server	https://www.se.com/de/de/product/MEG6501-0001/u.motion-knx-server/?range=63609-merten-knx-systeme&node=12366818621-knx-systemger%C3%A4te
MEG6501-0002 - U.motion KNX Server Plus	https://www.se.com/de/de/product/MEG6501-0002/u.motion-knx-server-plus/?range=63609-merten-knx-systeme&node=12366818621-knx-systemger%C3%A4te#pdp-download
MEG6260-0410 - U.motion KNX Server Plus, Touch 10	https://www.se.com/de/de/product/MEG6260-0410/u.motion-knx-server-plus%2C-touch-10/?range=63609-merten-knx-systeme&node=12366818621-knx-systemger%C3%A4te#pdp-download
MEG6260-0415 - U.motion KNX Server Plus, Touch 15	https://www.se.com/de/de/product/MEG6260-0415/u.motion-knx-server-plus%2C-touch-15/?range=63609-merten-knx-systeme&node=12366818621-knx-systemger%C3%A4te#pdp-download

The following workarounds and mitigations can be applied by customers to reduce the risk:

- Keep the U.motion server behind a firewall.
- Do not allow direct internet access to the U.motion server.

Product Information

U.motion Server is a residential and small business building management system.

Product Category - Residential and Small Business

Learn more about Schneider Electric's product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected

Any U.motion servers running versions older than 1.3.7 should upgrade to 1.3.7.

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.

Schneider Electric Security Notification

Acknowledgements

Schneider Electric recognizes the following researcher(s) for identifying and helping to coordinate a response to this vulnerability:

CVE	Researcher(s) Name
CVE-2019-6835, CVE-2019-6836, CVE-2019-6837	Zhu Jiaqi 诸嘉琦
CVE-2019-6840	Constantin-Cosmin Craciun

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

Legal Disclaimer

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, 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.

Schneider Electric Security Notification

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *10 Sep 2019*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2019.09.09 16:26:45 -04'00'