Schneider Electric Security Notification

U.motion Servers and Touch Panels V1.2

12 May 2020 (15 April 2021)

Overview

Schneider Electric is aware of multiple vulnerabilities in the U.motion servers and touch panel products.

Affected Products

All versions of the following:

- MTN6501-0001 – U.Motion – KNX Server
- MTN6501-0002 – U.Motion – KNX Server Plus
- MTN6260-0410 – U.Motion KNX server Plus, Touch 10
- MTN6260-0415 – U.Motion KNX server Plus, Touch 15
- MTN6260-0310 – U.Motion KNX Client Touch 10
- MTN6260-0315 – U.Motion KNX Client Touch 15

Vulnerability Details

CVE ID: **CVE-2020-7499**

CVSS v3.0 Base Score 6.3 | Medium | CVSS:3.0/AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:H/A:N]

A CWE-863: Incorrect Authorization vulnerability exists which could cause unauthorized access when a low privileged user makes unauthorized changes.

CVE ID: **CVE-2020-7500**

CVSS v3.0 Base Score 6.3 | Medium | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

A CWE-89:Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability exists which could cause arbitrary code to be executed when a malicious command is entered.

Remediation

These vulnerabilities are fixed in version 1.4.2 and are available for download below:

Affected Product	Fixed Version Download Link
MTN6501-0001 – U.motion – KNX Server https://www.se.com/ww/en/product/MTN6501-0001/u.motion---knx-server/	https://www.se.com/ww/en/product/MTN6501-0001/u.motion---knx-server/?range=61124-u.motion&node=827505925-server&parent-category-id=2200&parent-subcategory-id=88006 - pdp-software
MTN6501-0002 – U.Motion – KNX Server Plus https://www.se.com/ww/en/product/MTN6501-0002/u.motion---knx-server-plus/	https://www.se.com/ww/en/product/MTN6501-0002/u.motion---knx-server-plus/?range=61124-u.motion&node=827505925-server&parent-category-id=2200&parent-subcategory-id=88006 - pdp-software
MTN6260-0410 – U.Motion KNX server Plus, Touch 10 https://www.se.com/ww/en/product/MTN6260-0410/	https://www.se.com/ww/en/product/MTN6260-0410/u.motion-knx-server-plus,-touch-10/#pdp-software
MTN6260-0415 – U.Motion KNX server Plus, Touch 15 https://www.se.com/ww/en/product/MTN6260-0415/	https://www.se.com/ww/en/product/MTN6260-0415/u.motion-knx-server-plus,-touch-15/#pdp-software
MTN6260-0310 – U.Motion KNX Client Touch 10 https://www.se.com/ww/en/product/MTN6260-0310/	https://www.se.com/ww/en/product/MTN6260-0310/u.motion-client-touch-10/#pdp-software
MTN6260-0315 – U.Motion KNX Client Touch 15 https://www.se.com/ww/en/product/MTN6260-0315/	https://www.se.com/ww/en/product/MTN6260-0315/u.motion-client-touch-15/#pdp-software

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

- Do not allow direct internet access to the U.motion servers and touch panels.
- Keep the U.motion servers and touch panels behind a firewall.

Product Information

The U.motion servers and touch panels are a web-based visualization system for home and building automation based on KNX.

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 and touch panels running versions older than 1.4.2

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Put physical controls in place so no unauthorized person can access the ICS and safety controllers, peripheral equipment, or the ICS and safety networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.
- Never allow laptops that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and 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). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

Acknowledgements

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

CVE	Researcher(s) Name
CVE-2020-7499	Zhu Jiaqi
CVE-2020-7500	Rgod working with TrendMicro's Zero Day Initiative

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

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. 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

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, 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 about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *12 May 2020*	Original Release
Version 1.1 *19 May 2020*	Updated Acknowledgements section (page 4).
Version 1.2 *15 April 2021*	Updated CWE for CVE-2020-7499

Product Security Office Digitally signed by Product Security Office
Date: 2021.04.16 17:18:29 -04'00'