Life Is On | Schneider Electric

Schneider Electric Security Notification

Merten KNX devices

14 February 2023

Overview

Schneider Electric is aware of a vulnerability in its Merten KNX products.

The Merten KNX products in the table below are home automation products for lighting and temperature control.

Failure to apply the mitigations provided below may risk an authentication attack against the BCU Key, which could result in a compromised product.

Affected Products and Versions

Product	Version
Merten INSTABUS Tastermodul 1fach System M 625199	Program Version 1.0
Merten INSTABUS Tastermodul 2fach System M 625299	Program Version 1.0
Merten Tasterschnittstelle 4fach plus 670804	Program Version 1.0 Program Version 1.2
Merten KNX ARGUS 180/2,20M UP SYSTEM 631725	Program Version 1.0
Merten Jalousie-/Schaltaktor REG-K/8x/16x/10 m. HB 649908 (Product discontinued)	Program Version 1.0
Merten KNX Uni-Dimmaktor LL REG-K/2x230/300 W MEG6710-0002 (Product discontinued)	Program Version 1.0 Program Version 1.1
Merten KNX Schaltakt.2x6A UP m.2 Eing. MEG6003-0002 (Product discontinued)	Program Version 0.1

Vulnerability Details

CVE ID: **CVE-2023-25556**

CVSS v3.1 Base Score 8.3 | High | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

A *CWE-287: Improper Authentication* vulnerability exists that could allow a device to be compromised when a key of less than seven digits is entered and the attacker has access to the KNX installation.

Schneider Electric Security Notification

Mitigation

Product	Version	Mitigation
Merten **INSTABUS Tastermodul 1fach System M** 625199	Program Version 1.0	Customers must request their system integrator to increase their BCU Key to 8 digits.
Merten **INSTABUS Tastermodul 2fach System M** 625299	Program Version 1.0	
Merten **Tasterschnittstelle 4fach plus** 670804	Program Version 1.0 Program Version 1.2	
Merten **KNX ARGUS 180/2,20M UP SYSTEM** 631725	Program Version 1.0	
Merten **Jalousie-/Schaltaktor REG-K/8x/16x/10 m. HB** 649908 (Product discontinued)	Program Version 1.0	
Merten **KNX Uni-Dimmaktor LL REG-K/2x230/300 W** MEG6710-0002 (Product discontinued)	Program Version 1.0 Program Version 1.1	
Merten **KNX Schaltakt.2x6A UP m.2 Eing.** MEG6003-0002 (Product discontinued)	Program Version 0.1	

Customers should immediately apply the following mitigation to reduce the risk of exploit:

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.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and 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 intended for that device.
- 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 mobile devices 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.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

Acknowledgements

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

CVE	Researcher
CVE-2023-25556	Malte Küppers (FH Aachen - University of Applied Sciences)

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, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page: https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE 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 OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, 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. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY

Schneider Electric Security Notification

RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION

About Schneider Electric

Schneider's purpose is to empower all to make the most of our energy and resources, bridging progress and sustainability for all. We call this Life Is On.

Our mission is to be your digital partner for Sustainability and Efficiency.

We drive digital transformation by integrating world-leading process and energy technologies, end-point to cloud connecting products, controls, software and services, across the entire lifecycle, enabling integrated company management, for homes, buildings, data centers, infrastructure and industries.

We are the most local of global companies. We are advocates of open standards and partnership ecosystems that are passionate about our shared Meaningful Purpose, Inclusive and Empowered values.
www.se.com

Revision Control:

Version 1.0 *14 February 2023*	Original Release