Schneider Electric Security Notification

Harmony® eXLhoist

11 August 2020

Overview

Schneider Electric is aware of the Bluetooth Low Energy vulnerability, known as SweynTooth, which affects the Harmony® eXLhoist product.

Affected Product(s)

Harmony® eXLhoist base stations v04.00.02.00 and prior:

- ZARB12W
- ZARB12H
- ZARB18H
- ZARB18W
- ZARB18HM
- ZARB18WM

Note: Harmony® eXLhoist base stations compact range are not affected by this vulnerability.

Vulnerability Details

CVE ID: **CVE-2019-19193**

CVSS v3.1 Base Score 6.5 | Medium | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

The Bluetooth Low Energy peripheral implementation on Texas Instruments SIMPLELINK-CC2640R2-SDK through 3.30.00.20 and BLE-STACK through 1.5.0 before Q4 2019 for CC2640R2 and CC2540/1 devices does not properly restrict the advertisement connection request packet on reception, allowing attackers in radio range to cause a denial of service (crash) via a crafted packet.

Remediation

This vulnerability is fixed in base station V04.00.03.00 and is available for download below:

https://www.se.com/fr/fr/download/document/eXLhoistFirmwareV4060/

Product Information

The Harmony® eXLhoist range of wireless remote control systems is an operator control station used in hoisting and material handling applications

Product Category - Industrial Automation Control

Learn more about Schneider Electric's product categories here: https://www.se.com/us/en/all-products

How to determine if you are affected

Turn the eXLHoist system on, establish a connection between the base station and the remote control. Press in a sequence: Top and bottom buttons at the same time, then left and right buttons at the same time. The remote firmware version appears on the remote control screen. Press the right button to access the second page in order to see the base station version.

All versions up to V04.00.02.00 are affected.

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 to prevent unauthorized personnel from accessing 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 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 been connected to any network other than the intended network to connect to the intended networks without proper sanitation.
- Minimize network exposure to all control 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

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.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/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.

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 *11 August 2020*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2020.08.08 18:33:34 -04'00'