Schneider Electric Security Notification

Harmony (formerly known as Magelis) HMI Panels V1.1

13 August 2019 (11 August 2020)

Overview

Schneider Electric is aware of a vulnerability in the Harmony (formerly known as Magelis) HMI Panel products.

Affected Product(s)

- Vijeo Designer V6.2 SP9 or prior running on:
  - Harmony (formerly known as Magelis) HMIGTO series
  - Harmony (formerly known as Magelis) HMISTO series
  - Harmony (formerly known as Magelis) XBTGH series
  - Harmony (formerly known as Magelis) HMIGTU series
  - Harmony (formerly known as Magelis) HMIGTUX series
  - Harmony (formerly known as Magelis) HMISCU series
  - Harmony (formerly known as Magelis) HMISTU series
  - Magelis XBTGT series
  - Magelis XBTGC series
  - Magelis HMIGXO series
  - Magelis HMIGXU series

Vulnerability Details

CVE ID: **CVE-2019-6833**

CVSS v3.0 Base Score 7.4 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:N/A:H

A CWE-754 – Improper Check for Unusual or Exceptional Conditions vulnerability exists which could cause a temporary freeze of the HMI when a high rate of frames is received. When the attack stops, the buffered commands are processed by the HMI panel.

Remediation

Vijeo Designer V6.2 SP10 was released in the middle of July 2020. This new version includes the ability to disable the FTP Server (this is the behavior by default).

- For customers using Vijeo Designer version V6.1 or earlier, please contact your Schneider Electric Customer Support to obtain the Vijeo Designer V6.2 SP10.

- For customers using a version of Vijeo Designer V6.2 or greater, Vijeo Designer 6.2 SP10 will be automatically available in Schneider Electric Software Update (SESU) software.

Customers are urged to follow the Recommended Cybersecurity Best Practices found here https://www.se.com/ww/en/download/document/CS-Best-Practices-2019-340/ and to deactivate the FTP server.

Customers are also strongly encouraged to implement the following workarounds and mitigations to reduce the risk:

- Setup network segmentation and implement a firewall to block all unauthorized access to ports 44818/TCP, 502/TCP, 6000/TCP, 6002/TCP, 8080/TCP, 8014/TCP, and 6001/TCP.

Product Information

Harmony (formerly known as Magelis) HMI Panels are the main visible automation component that manage all vital machine features, including visualization, control, supervision, diagnostics, monitoring, and data logging.

Product Category - All Categories

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

How to determine if you are affected

Customers using Vijeo Designer V6.2 SP9 or prior running on the affected product references connected to an Ethernet network.

Note: General Tab - Contains the Vijeo Designer logo, name of the software, version number, and copyright information. Harmony HMI panels also display the version number at boot time.

General Security Recommendations

Schneider Electric Security Notification

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.
- Install physical controls to prevent unauthorized personnel from accessing your industrial control and safety systems, components, peripheral equipment, and networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- Never connect programming software to any network other than the target network.
- 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.
- 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), 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.

Acknowledgements

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

CVE	Researcher(s) Name
CVE-2019-6833	VAPT Team (C3i IITK, UP, India) Jie Chen (NSFOCUS)

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

Schneider Electric Security Notification

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 **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.

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 *13 August 2019*	Original Release
Version 1.1 *11 August 2020*	Updated Remediation and Acknowledgement sections (page 2 and 3)

Product Security Office

Digitally signed by Product Security Office
Date: 2020.08.10 11:36:17 -04'00'