

# Schneider Electric Security Notification

## Magelis HMI Panels

13 August 2019

### Overview

Schneider Electric is aware of a vulnerability in the Magelis HMI Panel products.

### Affected Product(s)

- Magelis HMIGTO series - all firmware versions
- Magelis HMISTO series - all firmware versions
- Magelis XBTGH series - all firmware versions
- Magelis HMIGTU series - all firmware versions
- Magelis HMIGTUX series - all firmware versions
- Magelis HMISCU series - all firmware versions
- Magelis HMISTU series - all firmware versions
- Magelis XBTGT series - all firmware versions
- Magelis XBTGC series - all firmware versions
- Magelis HMIGXO series - all firmware versions
- Magelis HMIGXU series - all firmware versions

### 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

Customers are 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.

# Schneider Electric Security Notification

## Product Information

Magelis HMI Panels are the main visible automation part which manages 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](http://www.schneider-electric.us/en/all-products)

### How to determine if you are affected

Magelis HMI Panel product references affected connected to an Ethernet network

## 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-2019-6833	VAPT Team (C3i IITK, UP, India)

## 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 **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](http://www.se.com)

# Schneider Electric Security Notification

Revision Control:

<b>Version 1</b> <i>13 Aug 2019</i>	Original Release
--	------------------