

Schneider Electric Security Notification

Harmony (formerly known as Magelis) HMI Panels

13 August 2019 (09 January 2024)

Overview

Schneider Electric is aware of a vulnerability in the Harmony (formerly known as Magelis) HMI Panel products. [Harmony HMI Panels](#) are the main visible automation component that manage all vital machine features, including visualization, control, supervision, diagnostics, monitoring, and data logging.

Failure to apply the mitigations/remediations provided below may risk a temporary Denial of Service.

January 2024 Update: A fix is available for *HMISCU* series.

Affected Products and Versions

| Product | Version |
|--|----------------------------|
| Harmony/Magelis HMIGK series | Version prior to v6.2 SP11 |
| Harmony/Magelis HMIGTO series | Version prior to v6.2 SP11 |
| Harmony/Magelis HMISTO series (End of Commercialization) | All versions |
| Harmony/Magelis) HMIGTU series | Version prior to v6.2 SP11 |
| Harmony/Magelis HMIGTUX series | Version prior to v6.2 SP11 |
| Harmony/Magelis HMIGXO series (End of Commercialization) | All versions |
| Harmony/Magelis HMIGXU series | All versions |
| Harmony/Magelis HMISCU series | Version prior to v6.3.1 |
| Harmony/Magelis HMISTU series | All versions |
| Harmony/Magelis XBTGC series | All versions |
| Harmony/Magelis XBTGH series | All versions |
| Harmony/Magelis XBTGT series (End of Commercialization) | All versions |

Schneider Electric Security Notification

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.

Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.0 without incorporating the Temporal and Environmental metrics. Schneider Electric recommends that customers score the CVSS Environmental metrics, which are specific to end-user organizations, and consider factors such as the presence of mitigations in that environment. Environmental metrics may refine the relative severity posed by the vulnerabilities described in this document within a customer's environment.

Remediation

| Affected Products | Remediation |
|--|---|
| Harmony/Magelis HMIGK series Harmony/Magelis HMIGTO series Harmony/Magelis HMIGTU series Harmony/Magelis HMIGTUX series <i>Versions prior to v6.2 SP11 HF4</i> | <p>Version 6.2 SP11 Multi HotFix 4 of Vijeo Designer includes a fix for these vulnerabilities and can be updated through the Schneider Electric Software Update (SESU) application.</p> <p>On the engineering workstation, update to v6.2 SP11 Multi HotFix 4 (or above) of Vijeo Designer.</p> <p>To complete the update, connect to Harmony HMI and download the project file using Vijeo Designer v6.2 SP11 Multi HotFix 4.</p> |
| Harmony/Magelis HMISCU series <i>Versions prior to v6.3.1</i> | <p>Version 6.3.1 of Vijeo Designer includes a fix for this vulnerability and can be updated through the Schneider Electric Software Update (SESU) application.</p> <p>https://www.se.com/ww/en/product-range/1054-vijeo-designer-hmi-software/#software-and-firmware</p> <p>On the engineering workstation, update to v6.3.1 of Vijeo Designer.</p> <p>To complete the update, connect to Harmony HMI and download the project file using Vijeo Designer v6.3.1.</p> |

Schneider Electric Security Notification

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's [Customer Care Center](#) if you need assistance removing a patch.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit.

Affected Products and Mitigations

| Affected Products | Mitigations |
|---|---|
| Harmony/Magelis HMIGK series Harmony/Magelis HMIGTO series Harmony/Magelis HMIGTU series Harmony/Magelis HMIGTUX series <i>Versions prior to v6.2 SP11 HF4</i> Harmony/Magelis HMISCU series <i>Versions prior to v6.3.1</i> | Customers should immediately apply the following mitigations below the table to reduce the risk of exploit. |
| Harmony/Magelis HMIGXU series Harmony/Magelis HMISTU series Harmony/Magelis XBTGC series Harmony/Magelis XBTGH series <i>All versions</i> | Customers should immediately apply the following mitigations below the table to reduce the risk of exploit. |
| Harmony/Magelis HMIGXO series Harmony/Magelis HMISTO series Harmony/Magelis XBTGT series <i>All versions</i> | <p>These products have reached their End of Commercialization.</p> <p>Customers should immediately apply the following mitigations below the table to reduce the risk of exploit or contact your Schneider Electric Customer Support to obtain its successor.</p> |

Recommended Mitigations

- Vijeo Designer v6.2 SP10 release 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 latest version of Vijeo Designer.

Schneider Electric Security Notification

- 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](#) 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.

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:

Schneider Electric Security Notification

| CVE | Researcher |
|---------------|---|
| 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, 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 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.

Schneider Electric Security Notification

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 1.0.0 13 August 2019 | Original Release |
| Version 1.1.0 11 August 2020 | Updated Remediation and Acknowledgement sections (page 2 and 3) |
| Version 2.0.0 08 February 2022 | A fix is available for <i>Harmony/Magelis HMIGTO series, Harmony/Magelis, HMIGTU series, Harmony/Magelis HMIGTUX series, Harmony/Magelis HMIGK series</i> and mitigations were added to reduce the risk of exploit for the remaining affected products. |
| Version 3.0.0 09 January 2024 | A fix is available for <i>Harmony/Magelis HMISCU</i> |