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.

Customers using Vijeo Designer V6.2 SP11 HotFix 3 or prior running on the affected product references connected to an Ethernet network.

February 2022 Update: A fix is available for Harmony/Magelis HMIGTO series, Harmony/Magelis, HMIGTU series, Harmony/Magelis HMIGTUX series, Harmony/Magelis HMIGK series and mitigations were added to reduce the risk of exploit for the remaining affected products.

Affected Products

- Harmony/Magelis HMIGTO series
- Harmony/Magelis HMISTO series (End of Commercialization)
- Harmony/Magelis XBTGH series
- Harmony/Magelis) HMIGTU series
- Harmony/Magelis HMIGTUX series
- Harmony/Magelis HMIGK series
- Harmony/Magelis HMISCU series
- Harmony/Magelis HMISTU series
- Harmony/Magelis XBTGT series (End of Commercialization)
- Harmony/Magelis XBTGC series
- Harmony/Magelis HMIGXO series (End of Commercialization)
- Harmony/Magelis HMIGXU series

Note: regarding offers End of Commercialization, please refer to below “Mitigations”.

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.
## Affected Products and Remediation

Vijeo Designer V6.2 SP11 multi HotFix 4 includes a fix for this vulnerability.

<table>
<thead>
<tr>
<th>Affected Products</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Harmony/Magelis HMIGTO series</td>
<td>Version V6.2 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. On the engineering workstation, update to V6.2 SP11 Multi HotFix 4 (or above) of Vijeo Designer. In order to complete the update, connect to Harmony HMI and download the project file using Vijeo Designer V6.2 SP11 Multi HotFix 4.</td>
</tr>
<tr>
<td>Harmony/Magelis HMIGTU series</td>
<td></td>
</tr>
<tr>
<td>Harmony/Magelis HMIGTUX series</td>
<td></td>
</tr>
<tr>
<td>Harmony/Magelis HMIGK series</td>
<td></td>
</tr>
</tbody>
</table>

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 mitigations below to reduce the risk of exploit.

## Affected Products and Mitigations

<table>
<thead>
<tr>
<th>Affected Products</th>
<th>Mitigations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Harmony/Magelis HMISCU series</td>
<td>Schneider Electric is establishing a remediation plan for a future version that will include a fix for this vulnerability. Customers should immediately apply the following mitigations to reduce the risk of exploit.</td>
</tr>
<tr>
<td>Harmony/Magelis HMISTU series</td>
<td>Customers should immediately apply the following mitigations to reduce the risk of exploit.</td>
</tr>
<tr>
<td>Harmony/Magelis XBTGH series</td>
<td></td>
</tr>
<tr>
<td>Harmony/Magelis XBTGC series</td>
<td></td>
</tr>
<tr>
<td>Harmony/Magelis HMIXU series</td>
<td></td>
</tr>
<tr>
<td>Harmony/Magelis HMISTO series</td>
<td>These products have reached their End of Commercialization. Customers should immediately apply the following mitigations to reduce the risk of exploit or contact your <a href="#">Schneider Electric Customer Support</a> to obtain its successor.</td>
</tr>
<tr>
<td>Harmony/Magelis XBTGT series</td>
<td></td>
</tr>
<tr>
<td>Harmony/Magelis HMIXO series</td>
<td></td>
</tr>
</tbody>
</table>
Recommended Mitigations

- Vijeo Designer V6.2 SP10 was released in the middle of July 2020. This 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 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 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 21/TCP, 44818/TCP, 502/TCP, 6000/TCP, 6002/TCP, 8080/TCP, 8014/TCP, and 6001/TCP.

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.
- 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 researchers for identifying and helping to coordinate a response to this vulnerability:

<table>
<thead>
<tr>
<th>CVE</th>
<th>Researchers</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2019-6833</td>
<td>VAPT Team (C3i IITK, UP, India) and Jie Chen (NSFOCUS)</td>
</tr>
</tbody>
</table>

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

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:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1</td>
<td>13 August 2019</td>
<td>Original Release</td>
</tr>
<tr>
<td>Version 1.1</td>
<td>11 August 2020</td>
<td>Updated Remediation and Acknowledgement sections (page 2 and 3)</td>
</tr>
<tr>
<td>Version 2.0</td>
<td>8 February 2022</td>
<td>A fix is available for Harmony/Magelis HMIGTO series, Harmony/Magelis, HMIGTU series, Harmony/Magelis HMIGTUX series, Harmony/Magelis HMIGK series and mitigations were added to reduce the risk of exploit for the remaining affected products.</td>
</tr>
</tbody>
</table>

### Product Security Office

Digitally signed by Product Security Office  
Date: 2022.02.10 13:58:33 -08'00'