Schneider Electric Security Notification

Harmony/Magelis HMI Products configured by Vijeo Designer, Vijeo Designer Basic and EcoStruxure Machine Expert

10 August 2021

Overview

Schneider Electric is aware of a vulnerability in Harmony HMI Products configured by Vijeo Designer, Vijeo Designer Basic and EcoStruxure Machine Expert.

The Harmony HMI products are configured by Vijeo Designer software, Vijeo Designer Basic or EcoStruxure Machine Expert. These are software solutions for developing, configuring, and commissioning an entire machine in a single software environment.

Failure to apply the remediations provided below may risk unauthorized access through FTP protocol, which could result in a Denial of Service or tampering with systems files on the Harmony HMI.

Affected Products and Versions

Product	Configuration Software
Harmony/Magelis STO	Configured with Vijeo Designer – all versions prior to V6.2 SP11
Harmony/Magelis STU	
Harmony/Magelis GTO	
Harmony/Magelis GTU	
Harmony/Magelis GTUX	
Harmony/Magelis GK	
Harmony/Magelis GXU	Configured with Vijeo Designer Basic – all versions prior to V1.2
Harmony/Magelis SCU	Configured with EcoStruxure™ Machine Expert – all versions prior to V2.0

Vulnerability Details

CVE ID: **CVE-2021-22704**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A CWE-22: *Improper Limitation of a Pathname to a Restricted Directory* vulnerability exists that could cause a Denial of Service or unauthorized access to system information when connecting to the Harmony HMI over FTP.

Remediation

Configuration Software	Remediation
Vijeo Designer – all versions prior to V6.2 SP11	1. On the engineering workstation, update to V6.2 SP11 (or above) of Vijeo Designer which includes a fix for this vulnerability and is available for download here: https://www.se.com/ww/en/product-range/1054-vijeo-designer/?parent-subcategory-id=82307&filter=business-1-industrial-automation-and-control&selected-node-id=12146993558#software-and-firmware 2. Connect to Harmony HMI and download the project file using Vijeo Designer V6.2 SP11
Vijeo Designer Basic – all versions prior to V1.2	1. Vijeo Designer Basic V1.2 includes a fix for this vulnerability. Please contact your Schneider Electric Customer Care Center to obtain the installer. 2. Connect to Harmony HMI and download the firmware using Vijeo Designer Basic V1.2.
EcoStruxure™ Machine Expert – all versions prior to V2.0	1. On the engineering workstation, update to EcoStruxure Machine Expert V2.0 or above: https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-%28somachine%29/?selected-node-id=14435955187#software-and-firmware 2. On the HMISCU Logic Controller, update to latest firmware version available within EcoStruxure™ Machine Expert V2.0.

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:

- Follow Online Help of "4.8.2.2 Protecting Targets from Unauthorized Project Downloads" to enable FTP protection, which is installed on the user workstation.
    - In the Security editor, enter the username and password and use the Download Access drop-down list to select Allowed for the security group.

- Setup network segmentation and implement a firewall to block all unauthorized access to port TCP/6001 (Not standard FTP port).
- Use Vijeo Designer, Vijeo Designer Basic, EcoStruxure™ Machine Expert V2.0 software and Harmony HMIs only on a trusted network.
- Harden your network and Harmony Product following the best cybersecurity practices (antivirus, updated operating systems, strong password policies, application white listing software, etc.) using the Recommended Cybersecurity Best Practices document.

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 for the devices 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 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:

CVE	Researcher
CVE-2021-22704	Jie Chen (NSFOCUS)

Schneider Electric Security Notification

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. 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 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

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 1.0 *10 August 2021*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2021.08.09 09:32:21 -04'00'