

Schneider Electric Security Notification

Harmony/Magelis iPC Series HMI, Vijeo Designer and Vijeo Designer Basic

08 February 2022

Overview

Schneider Electric is aware of a vulnerability in Harmony/Magelis iPC Series HMI, Vijeo Designer and Vijeo Designer Basic.

The [Harmony/Magelis iPC Series HMI](#) products are configured by [Vijeo Designer](#) software. Vijeo Designer and Vijeo Designer Basic 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 to the base installation directory due to improper access control lists, which could result in local privilege escalation.

Affected Products and Versions

Product	Version
Harmony/Magelis iPC Series	All Versions
Vijeo Designer	All Versions prior to V6.2 SP11 Multiple HotFix 4
Vijeo Designer Basic	All Versions prior to V1.2.1

Vulnerability Details

CVE ID: **CVE-2021-22817**

CVSS v3.1 Base Score 7.1 | High | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

A *CWE-276: Incorrect Default Permissions* vulnerability exists that could cause unauthorized access to the base installation directory leading to local privilege escalation.

Schneider Electric Security Notification

Remediations

Product	Remediation
Harmony/Magelis iPC Series	<p>Version V6.2 SP11 Multi HotFix 4 of Vijeo Designer includes a fix for this vulnerability 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>In order to complete the update, connect to Harmony iPC Series HMI and download the project file using Vijeo Designer V6.2 SP11 Multi HotFix 4.</p>
Vijeo Designer V6.2 SP11 Multi HotFix 4	<p>Version V6.2 SP11 Multi HotFix 4 of Vijeo Designer includes a fix for this vulnerability 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>
Vijeo Designer Basic V1.2.1	<p>Version v1.2.1 of Vijeo Designer Basic includes a fix for this vulnerability.</p> <p>Please contact your Schneider Electric Customer Care Center to obtain the installer.</p>

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:

- Install physical controls so no unauthorized personnel can access your HMI Device, Laptop, and engineering workstation.
- 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.

Schneider Electric Security Notification

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:

CVE	Researcher
CVE-2021-22817	Sharon Brizinov (Claroty)

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.

Schneider Electric Security Notification

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

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 08 February 2022	Original Release
--	-------------------------