# Schneider Electric Security Notification

## CODESYS Runtime Vulnerabilities

**11 July 2023 (9 April 2024)**

## Overview

Schneider Electric is aware of multiple vulnerabilities disclosed on CODESYS runtime system V3 communication server. Many vendors, including Schneider Electric, embed CODESYS in their offers.

If successfully exploited, these vulnerabilities could result in a denial of service or, in some cases, in remote code execution on PacDrive controllers, Modicon Controllers M241 / M251 / M262 / M258 / LMC058 / LMC078 / M218, HMISCU, and the Simulation Runtime SoftSPS & Vijeo Designer embedded in EcoStruxure Machine Expert products, Harmony HMIGK/HMIGTO/HMIGTU/HMIGTUX/HMISTU series, iPC series, Easy Harmony HMIET6/HMIFT6, and Magelis HMIGXU, XBT series.

Failure to apply the mitigations provided below may result in denial of service and/or arbitrary remote code execution.

April 2024 Update: A remediation is now available for Easy Harmony HMIET6/HMIFT6, and Magelis HMIGXU series (page 3).

## Details

Vulnerabilities disclosed by CODESYS™ group in the CODESYS Runtime and Simulation Runtime impact Schneider Electric controller products and software.

Additional information about the vulnerabilities can be found in the CODESYS™ Advisories at:

- Advisory 2023-02
- Advisory 2023-03
- Advisory 2023-04
- Advisory 2023-05
- Advisory 2023-06
- Advisory 2023-07
- Advisory 2023-08
- Advisory 2023-09

# Schneider Electric Security Notification

## Affected Products and Versions

| Product | Version |
|---|---|
| Easy Harmony HMIET6/HMIFT6<br>Magelis HMIGXU | All versions prior to v2.0 HF2 |
| Harmony (Formerly Magelis)<br>HMIGK/HMIGTO/HMIGTU/HMIGTUX/HMISTU series, | All versions prior to V6.3 HF3 |
| Harmony<br>iPC series with Vijeo Designer runtime | All versions |
| HMISCU Controller | All versions prior to v6.3.1 |
| Magelis XBT series | All versions |
| Modicon Controller LMC078 | All versions |
| Modicon Controller M241 | All versions prior to v5.2.11.18 |
| Modicon Controller M251 | All versions prior to v5.2.11.18 |
| Modicon Controller M262 | All versions prior to v5.2.8.12 |
| Modicon Controller M258 | All versions |
| Modicon Controller LMC058 | All versions |
| Modicon Controller M218 | All versions |
| PacDrive 3 Controllers: LMC Eco/Pro/Pro2 | All versions prior to v1.76.14.1 |
| SoftSPS embedded in EcoStruxure™ Machine Expert | All versions prior to Machine Expert v2.2 |
| Vijeo Designer embedded in EcoStruxure™ Machine Expert | All versions prior to v6.3.1 |

## Remediation

**We encourage customers to apply the remediations provided and the mitigations detailed here below to reduce the risk of exploit. Please note that Advisory-2023-04 vulnerability can only be mitigated.**

| Affected Product & Version | Remediation | Remediated Advisory |
|---|---|---|
| **Easy Harmony HMIET6/HMIFT6 Magelis HMIGXU** *All versions prior to v2.0 HF2* | Vijeo Designer Basic v2.0 HotFix 2 includes a fix for this vulnerability. Please contact your Schneider Electric Customer Care Center to obtain the installer.<br><br>To complete the update, connect to Harmony HMI and download the firmware using Vijeo Designer Basic. | Advisory 2023-02<br>Advisory 2023-03<br>Advisory 2023-05<br>Advisory 2023-06<br>Advisory 2023-07<br>Advisory 2023-08<br>Advisory 2023-09 |
| **Harmony (Formerly Magelis) HMIGK/HMIGTO/HMIGTU/HMIGTUX/HMISTU series** *All versions prior to v6.3 HF3* | Version 6.3 HF3 of Vijeo Designer includes a fix for this vulnerability and can be updated through the Schneider Electric Software Update (SESU) application.<br><br>As an alternative, please contact your Schneider Electric Customer Care Center to obtain the Hot Fix. For additional detail please refer to the supplied help file in Hot Fix.<br><br>On the engineering workstation, update to v6.3 HF3 of Vijeo Designer. | Advisory 2023-02<br>Advisory 2023-03<br>Advisory 2023-05<br>Advisory 2023-06<br>Advisory 2023-07<br>Advisory 2023-08<br>Advisory 2023-09 |
| **HMISCU Controller** *All versions prior to v6.3.1* | 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.<br><br>https://www.se.com/ww/en/product-range/1054-vijeo-designer-hmi-software/#software-and-firmware<br><br>On the engineering workstation, update to v6.3.1of Vijeo Designer.<br><br>To complete the update, connect to Harmony HMI and download the project file using Vijeo Designer v6.3.1. | Advisory 2023-02<br>Advisory 2023-03<br>Advisory 2023-05<br>Advisory 2023-06<br>Advisory 2023-07<br>Advisory 2023-08<br>Advisory 2023-09 |
| **Magelis XBT series** *All versions* | Schneider Electric's Magelis XBT series have reached their end of commercialization. Magelis XBTGT/XBTGK offers have been replaced by HMIGTO/HMIGTU/HMIGK. We recommend our | Advisory 2023-02<br>Advisory 2023-03<br>Advisory 2023-05<br>Advisory 2023-06 |

| | | |
|---|---|---|
| | customers to migrate to the latest offers. For Magelis XBT series that haven't been replaced, please contact your local Schneider Electric technical support for more information. | Advisory 2023-07<br>Advisory 2023-08<br>Advisory 2023-09 |
| **Modicon Controller LMC078**<br>*All versions* | Schneider Electric's Modicon LMC078 controllers have reached end of their life and are no longer commercially available. They have been replaced by the Modicon M262 controllers. We recommend our customers to migrate to the latest offer. Please contact your local Schneider Electric technical support for more information. | Advisory 2023-02<br>Advisory 2023-03<br>Advisory 2023-04<br>Advisory 2023-05<br>Advisory 2023-06<br>Advisory 2023-07<br>Advisory 2023-08<br>Advisory 2023-09 |
| **Modicon Controller M218**<br>*All versions* | Schneider Electric's Modicon M218 controllers have reached their end of life and are no longer commercially available. They have been replaced by the Modicon Easy M200 and Modicon M241 controllers. We recommend our customers to migrate to the latest offer. Please contact your local Schneider Electric technical support for more information. | Advisory 2023-02<br>Advisory 2023-03<br>Advisory 2023-04<br>Advisory 2023-05<br>Advisory 2023-06<br>Advisory 2023-07<br>Advisory 2023-08<br>Advisory 2023-09 |
| **Modicon Controller M241**<br>*All versions prior to V5.2.11.18* | Modicon Controller M241 Firmware delivered with Machine Expert v2.2 includes a fix for this vulnerability and can be updated through the Schneider Electric Software Update (SESU) application.<br><br>https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-software/<br><br>On the engineering workstation, update to v2.2 of Machine Expert.<br><br>Update Modicon Controller M241 to the latest Firmware and preform reboot. | Advisory 2023-02<br>Advisory 2023-03<br>Advisory 2023-05<br>Advisory 2023-06<br>Advisory 2023-07<br>Advisory 2023-08<br>Advisory 2023-09 |
| **Modicon Controller M251**<br>*All versions prior to v5.2.11.18* | Modicon Controller M251 Firmware delivered with Machine Expert v2.2 includes a fix for this vulnerability and can be updated through the Schneider Electric Software Update (SESU) application.<br><br>https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-software/<br><br>On the engineering workstation, update to v2.2 of Machine Expert.<br><br>Update Modicon Controller M251 to the latest Firmware and preform reboot. | Advisory 2023-02<br>Advisory 2023-03<br>Advisory 2023-05<br>Advisory 2023-06<br>Advisory 2023-07<br>Advisory 2023-08<br>Advisory 2023-09 |

| | | |
|---|---|---|
| **Modicon Controller M262**<br>*All versions prior to v5.2.8.12* | Modicon Controller M262 Firmware delivered with Machine Expert v2.2 includes a fix for this vulnerability and can be updated through the Schneider Electric Software Update (SESU) application.<br><br>https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-software/<br><br>On the engineering workstation, update to v2.2 of Machine Expert.<br><br>Update Modicon Controller M262 to the latest Firmware and preform reboot. | Advisory 2023-02<br>Advisory 2023-03<br>Advisory 2023-05<br>Advisory 2023-06<br>Advisory 2023-07<br>Advisory 2023-08<br>Advisory 2023-09 |
| **PacDrive 3 Controller: LMC Eco/Pro/Pro2**<br>*All versions prior to v1.76.14.1* | PacDrive 3 Controllers LMC Eco/Pro/Pro2 Firmware delivered with Machine Expert V2.2 includes a fix for this vulnerability and can be updated through the Schneider Electric Software Update (SESU) application.<br><br>https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-software/<br><br>On the engineering workstation, update to V2.2 of Machine Expert.<br><br>Update PacDrive 3 Controllers: LMC Eco/Pro/Pro2 to the latest Firmware and preform reboot. | Advisory 2023-02<br>Advisory 2023-03<br>Advisory 2023-05<br>Advisory 2023-06<br>Advisory 2023-07<br>Advisory 2023-08<br>Advisory 2023-09 |
| **SoftSPS embedded in EcoStruxure ™ Machine Expert**<br>*All versions prior to v2.2* | SoftSPS component has been removed from Machine Expert V2.2. Machine Expert can be updated through the Schneider Electric Software Update (SESU) application.<br><br>https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-software/ | Advisory 2023-02<br>Advisory 2023-03<br>Advisory 2023-05<br>Advisory 2023-06<br>Advisory 2023-07<br>Advisory 2023-08<br>Advisory 2023-09 |
| **Vijeo Designer embedded in EcoStruxur™ Machine Expert**<br>*All versions prior to v6.3.1* | 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.<br><br>https://www.se.com/ww/en/product-range/1054-vijeo-designer-hmi-software/#software-and-firmware<br><br>On the engineering workstation, update to v6.3.1of Vijeo Designer. | Advisory 2023-02<br>Advisory 2023-03<br>Advisory 2023-05<br>Advisory 2023-06<br>Advisory 2023-07<br>Advisory 2023-08<br>Advisory 2023-09 |

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.

## Mitigations

| Affected Product & Version | Mitigations |
|---|---|
| **HMISCU Controller**<br>**Modicon Controller LMC078**<br>**Modicon Controller M241**<br>**Modicon Controller M251**<br>**Modicon Controller M262**<br>**Modicon Controller M258**<br>**Modicon Controller LMC058**<br>**Modicon Controller M218**<br>**PacDrive 3 Controllers LMC Eco/Pro/Pro2**<br>*All versions*<br><br>**SoftSPS embedded in EcoStruxure Machine Expert**<br>*All versions prior to Machine Expert V2.2* | Customers should immediately apply the following mitigations to reduce the risk of exploitation:<br>• Ensure usage of user management and password features. User rights are enabled by default and forced to create a strong password at first use.<br>• Use encrypted communication links.<br>• The "Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment" provide mitigations through the activation of project encryption in the Enhanced Security Settings, chapter https://download.schneider-electric.com/files?p_enDocType=User+guide&p_File_Name=EIO0000004242.00.pdf&p_Doc_Ref=EIO0000004242.<br>• Restrict access to programming ports, typically UDP/1740, TCP/11740 and TCP/1105.<br>• Enable the optional 'Implicit Checks' on logic applications.<br>• Avoid use of the POINTER data type and MEMMOVE instructions, especially on untrusted inputs.<br>• Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside.<br>• Use firewalls to protect and separate the control system network from other networks.<br>• Use VPN (Virtual Private Networks) tunnels if remote access is required.<br>• Limit the access to both development and control system by physical means, operating system features, etc.<br>• Protect both development and control system by using up to date malware protection.<br><br>To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp |

| | |
|---|---|
| **Easy Harmony HMIET6/HMIFT6 series, Magelis HMIGXU**<br>*All versions prior to v2.0 HF2* | Customers should immediately apply the following mitigations to reduce the risk of exploitation:<br><br>• Ensure usage of user management and password features.<br>• Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside.<br>• Use firewalls to protect and separate the control system network from other networks.<br>• Use VPN (Virtual Private Networks) tunnels if remote access is required.<br>• Limit the access to both development and control system by physical means, operating system features, etc.<br>• Protect both development and control system by using up to date malware protection.<br><br>To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp |
| **Harmony iPC series with Vijeo Designer runtime**<br>*All versions* | Schneider Electric is establishing a remediation plan for all future versions that will include a fix for these vulnerabilities. We will update this document when the remediations are available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploitation.<br>• Ensure usage of user management and password features.<br>• Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside.<br>• Use firewalls to protect and separate the control system network from other networks.<br>• Use VPN (Virtual Private Networks) tunnels if remote access is required.<br>• Limit the access to both development and control system by physical means, operating system features, etc.<br>• Protect both development and control system by using up to date malware protection.<br><br>To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here: |

| | |
|---|---|
| | https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp |
| **Harmony (Formerly Magelis) HMIGK/HMIGTO/HMIGTU/HMIGTUX/HMISTU**<br>*All versions prior to v6.3 HF3*<br><br>**Magelis XBT series**<br>*All versions*<br><br>**Vijeo Designer embedded in EcoStruxure™ Machine Expert**<br>*All versions prior to v6.3.1* | Customers should immediately apply the following mitigations to reduce the risk of exploitation:<br><br>• Ensure usage of user management and password features.<br>• Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside.<br>• Use firewalls to protect and separate the control system network from other networks.<br>• Use VPN (Virtual Private Networks) tunnels if remote access is required.<br>• Limit the access to both development and control system by physical means, operating system features, etc.<br>• Protect both development and control system by using up to date malware protection.<br><br>To ensure you are informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service here: https://www.se.com/en/work/support/cybersecurity/security-notifications.jsp |

## 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.

## 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.

# Schneider Electric Security Notification

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.

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**<br>*11 July 2023* | Original Release |
| **Version 2.0.0**<br>*08 August 2023* | New CODESYS advisories 2023-04 to 2023-09 added. Additional impacted product: Harmony and Easy Harmony, Vijeo Designer embedded in EcoStruxure™ Machine Expert. |
| **Version 3.0.0**<br>*09 January 2024* | Remediations added for different products. |
| **Version 4.0.0**<br>*12 March 2024* | A remediation is now available for HMIGK/HMIGTO/HMIGTU/ HMIGTUX/HMISTU series (page 5). |
| **Version 5.0.0**<br>*09 April 2024* | A remediation is now available for Easy Harmony HMIET6/HMIFT6, and Magelis HMIGXU series (page 3). |

CPCERT

Digitally signed by CPCERT
Date: 2024.04.08 10:04:19 -04'00'