Schneider Electric Security Notification

CODESYS Runtime Vulnerabilities

11 April 2023 (09 January 2024)

Overview

Schneider Electric is aware of multiple vulnerabilities disclosed on CODESYS Runtime. 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 / M218 and HMISCU products.

Failure to apply the mitigations provided below may risk Logic Integrity and Permissions attacks, which could result in loss of controllers' integrity.

January 2024 Update: A remediation is available for CVE-2022-4224 for Harmony HMISCU Controller, Modicon Controllers M241 / M251 / M262 and PacDrive Controllers LMC Eco/Pro/Pro2.

Affected Products and Versions

Product	CVE-2022-4046 CVE-2023-28355	CVE-2022-4224
Harmony HMISCU Controller	All	All versions prior to v6.3.1
Modicon Controller LMC078	All	All
Modicon Controller M241 Modicon Controller M251	All	All versions prior to v5.2.11.18
Modicon Controller M262	All	All versions prior to v5.2.8.12
Modicon Controller M258 Modicon Controller LMC058	All	All
Modicon Controller M218	All	All
PacDrive 3 Controllers LMC Eco/Pro/Pro2	All	All versions prior to v1.76.14.1

Vulnerability Details

CODESYS have released a series of vulnerabilities affecting the CODESYS Runtime:

CVE ID: **CVE-2022-4224**

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-668: Exposure of Resource to Wrong Sphere* vulnerability exists that could cause inappropriate access to Sensitive System Files when user management is not configured.

CVE ID: **CVE-2022-4046**

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-119: Improper Restriction of Operations within the Bounds of a Memory Buffer* vulnerability exists that could cause loss of view, modification of view, loss of control, and denial of control when Integrity check fails to identify out-of-band logic changes.

CVE ID: **CVE-2023-28355**

CVSS v3.1 Base Score 7.7 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:H/A:N

A *CWE-354: Improper Validation of Integrity Check Value* vulnerability exists that could cause loss of view, modification of view, loss of control, and denial of control when Integrity check fails to identify out-of-band logic changes.

Note regarding vulnerability details: The severity of vulnerabilities was calculated using the CVSS Base metrics in version 3.1 (CVSS v3.1) 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 Product & Version	Remediation	CVEs
Harmony HMISCU Controller *All versions prior to v6.3.1*	Harmony HMISCU Controller Firmware delivered with Vijeo Designer v6.3.1 includes a fix for CVE-2022-4224 vulnerability and can be updated through the Schneider Electric Software Update (SESU) application. https://www.se.com/ww/en/product-range/1054-vijeo-designer-hmi-software/#software-and-firmware	CVE-2022-4224

	On the engineering workstation, update to v6.3.1 of Vijeo Designer. In order to complete the update, connect to Harmony HMI and download the project file using Vijeo Designer v6.3.1.	
Modicon Controller LMC078 *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.	CVE-2022-4046 CVE-2022-4224 CVE-2023-28355
Modicon Controller M218 *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.	CVE-2022-4046 CVE-2022-4224 CVE-2023-28355
Modicon Controller M241 *All versions prior to v5.2.11.18*	Modicon Controller M241 Firmware delivered with Machine Expert v2.2 includes a fix for CVE-2022-4224 vulnerability and can be updated through the Schneider Electric Software Update (SESU) application. https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-software/ On the engineering workstation, update to v2.2 of Machine Expert. Update Modicon Controller M241 to the latest Firmware and preform reboot.	CVE-2022-4224
Modicon Controller M251 *All versions prior to v5.2.11.18*	Modicon Controller M251 Firmware delivered with Machine Expert v2.2 includes a fix for CVE-2022-4224 vulnerability and can be updated through the Schneider Electric Software Update (SESU) application. https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-software/ On the engineering workstation, update to v2.2 of Machine Expert. Update Modicon Controller M251 to the latest Firmware and preform reboot.	CVE-2022-4224

Modicon Controller M262 *All versions prior to v5.2.8.12*	Modicon Controller M262 Firmware delivered with Machine Expert v2.2 includes a fix for CVE-2022-4224 vulnerability and can be updated through the Schneider Electric Software Update (SESU) application. https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-software/ On the engineering workstation, update to V2.2 of Machine Expert. Update Modicon Controller M262 to the latest Firmware and preform reboot.	CVE-2022-4224
PacDrive 3 Controllers LMC Eco/Pro/Pro2 *All versions prior to v1.76.14.1*	PacDrive3 Controllers LMC Eco/Pro/Pro2 Firmware delivered with Machine Expert v2.2 includes a fix for CVE-2022-4224 vulnerability and can be updated through the Schneider Electric Software Update (SESU) application. https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-software/ On the engineering workstation, update to v2.2 of Machine Expert. Update PacDrive 3 Controllers LMC Eco/Pro/Pro2 to the latest Firmware and preform reboot.	CVE-2022-4224

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.

To mitigate the remaining vulnerabilities or if customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

Mitigations

Affected Product & Version	Mitigations
PacDrive 3 Controllers LMC Eco/Pro/Pro2 **Modicon Controller LMC078** **Modicon Controller M241** **Modicon Controller M251** **Modicon Controller M262** **Modicon Controller M258** **Modicon Controller LMC058** **Modicon Controller M218** **HMISCU Controller** *All versions*	Please apply the following: - 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. - Restrict access to programming ports, typically UDP/1740, TCP/11740 and TCP/1105. - Enable the optional ‘Implicit Checks’ on logic applications. - Avoid use of the POINTER data type and MEMMOVE instructions, especially on untrusted inputs. - Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside. - Use firewalls to protect and separate the control system network from other networks. - Use VPN (Virtual Private Networks) tunnels if remote access is required. - Activate and apply user management and password features. - Use encrypted communication links. - Limit the access to both development and control system by physical means, operating system features, etc. - Protect both development and control system by using up to date malware protection. 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

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 these vulnerabilities:

CVE	Researcher
CVE-2022-4224 CVE-2022-4046 CVE-2023-28355	Reid Wightman (Dragos Inc.)

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

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.

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 *11 April 2023*	Original Release
Version 1.1.0 *13 April 2023*	Updated acknowledgement section
Version 2.0.0 *09 January 2024*	A remediation is now available for CVE-2022-4224 for Harmony HMISCU Controller HMISCU, Modicon Controllers M241 / M251 / M262 and PacDrive Controllers LMC Eco/Pro/Pro2.

Product Security Office

Digitally signed by Product Security Office
Date: 2024.01.08 13:42:08 -05'00'