Schneider Electric Security Notification

CODESYS V3 Runtime, Development System, and Gateway Vulnerabilities

11 January 2022 (11 April 2023)

Overview

Schneider Electric is aware of multiple vulnerabilities disclosed by Codesys on CODESYS V3 Runtime, Development System and Gateway. Many vendors, including Schneider Electric, embed CODESYS in their offers. If successfully exploited, these vulnerabilities could result in denial of service or, in some cases, remote code execution.

Customers should immediately ensure they have implemented cybersecurity best practices across their operations to protect themselves from possible exploitation of these vulnerabilities. Where appropriate, this includes locating their industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; preventing mission-critical systems and devices from being accessed from outside networks; and following the mitigations and general security recommendations below.

For additional information and support, please contact your Schneider Electric sales or service representative or Schneider Electric's Customer Care Center.

April 2023 Update: A remediation is available for Easy Harmony ET6 (HMIET Series) and Easy Harmony GXU (HMIGXU Series) (page 4).

Vulnerability Details

Codesys have released a series of vulnerabilities affecting the Codesys Runtime, Development System and Gateway components:

- Security update for CODESYS V3 web server
  - CVE-2021-33485
- Security update for CODESYS Gateway V3
  - CVE-2021-29241
- Security update for CODESYS Development System V3
  - CVE-2021-29240
  - CVE-2021-21863
  - CVE-2021-21864
  - CVE-2021-21865
  - CVE-2021-21866
  - CVE-2021-21867
  - CVE-2021-21868
  - CVE-2021-21869

Additional details on these vulnerabilities can be found in the CODESYS advisories linked above.

Affected Products and Remediations

Affected Product & Versions	CVEs	Remediations
EcoStruxure™ Machine Expert *Versions prior to V2.0.3*	CVE-2021-21863 CVE-2021-21864 CVE-2021-21865 CVE-2021-21866 CVE-2021-21867 CVE-2021-21868 CVE-2021-21869	Version 2.0.3 of EcoStruxure™ Machine Expert includes a fix for these vulnerabilities. On the engineering workstation, update to latest version of EcoStruxure™ Machine Expert: https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-somachine/?parent-subcategory-id=5140&filter=business-1-industrial-automation-and-control
Eurotherm E+PLC100 *All Versions*	CVE-2021-33485	E+PLC100 is no longer commercially available as of 2021. Customers should immediately apply the recommended mitigations provided below to reduce the risk of exploit and contact Eurotherm support team for advice about migrating to other Eurotherm offers.
Eurotherm E+PLC400 *V1.3.0.1 and prior*	CVE-2021-33485	Version 1.4.0.0 of the E+PLC400 firmware is available and includes a fix for this vulnerability. Please contact the Eurotherm Support team to obtain the firmware update. Please be sure to include the following when contacting the support team: • End Username, Company and Email Address • Serial numbers of the devices to be upgraded • Current E+PLC firmware version

Eurotherm E+PLC tools *V1.3.0.1 and prior*	CVE-2021-29240 CVE-2021-29241 CVE-2021-21863 CVE-2021-21864 CVE-2021-21865 CVE-2021-21866 CVE-2021-21867 CVE-2021-21868 CVE-2021-21869	Version 1.4.0.0 of the E+PLC Tools software is available and includes a fix for these vulnerabilities. Please contact the Eurotherm Support team to obtain the firmware update.
Modicon M241/M251 *Version prior to 5.1.9.34*	CVE-2021-29241 CVE-2021-33485	Version 5.1.9.34 of Modicon M241/M251 Logic Controllers includes a fix for these vulnerabilities. On the engineering workstation, update to latest version of EcoStruxure™ Machine Expert: https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-somachine/?parent-subcategory-id=5140&filter=business-1-industrial-automation-and-control To complete the update on Modicon M241/M251 Logic Controllers, update to firmware V5.1.9.34 or higher available within EcoStruxure™ Machine Expert. A reboot is needed.
Harmony/ Magelis HMISCU Series EcoStruxure™ Machine Expert *V2.0.3 and prior*	CVE-2021-29241	Version 2.1.0 of EcoStruxure™ Machine Expert includes a fix for this vulnerability. On the engineering workstation, update to latest version of EcoStruxure™ Machine Expert. To complete the update, connect to Harmony HMISCU and download the project file using EcoStruxure ™ Machine Expert. https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-somachine/?parent-subcategory-id=5140&filter=business-1-industrial-automation-and-control

Schneider Electric Security Notification

Harmony (formerly Magelis) HMISTU Series HMIGTO Series HMIGTU Series HMIGTUX Series HMIGK Series *Vijeo Designer V6.2 SP12 Hotfix 3 and prior*	CVE-2021-29241	Version V6.2 SP12 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 SP12 HotFix 4 (or above) of Vijeo Designer. To complete the update, connect to Harmony HMI and download the project file using Vijeo Designer V6.2 SP12 HotFix 4.
Easy Harmony ET6 (HMIET Series) *Vijeo Designer Basic V1.2.1 Hotfix 3 and prior*	CVE-2021-29241	Vijeo Designer Basic V1.2.1 HotFix 4 includes a fix for this vulnerability. Please contact your Schneider Electric Customer Care Center to obtain the installer. To complete the update, connect to Harmony HMI and download the firmware using Vijeo Designer Basic V1.2.1 HotFix 4.
Easy Harmony GXU (HMIGXU Series) *Vijeo Designer Basic V1.2.1 Hotfix 3 and prior*	CVE-2021-29241	Vijeo Designer Basic V1.2.1 HotFix 4 includes a fix for this vulnerability. Please contact your Schneider Electric Customer Care Center to obtain the installer. To complete the update, connect to Harmony HMI and download the firmware using Vijeo Designer Basic V1.2.1 HotFix 4.

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.

Schneider Electric Security Notification

Recommended Mitigations

Customers should immediately apply the following mitigations to reduce the risk of exploit:

- 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,
- Limit the access to both development and control system by physical means, operating system features, etc.

Subscribe to the Schneider Electric security notification service to be informed of critical updates to this notification, including information on affected products and remediation plans: https://www.se.com/ww/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.

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: 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

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

Schneider Electric Security Notification

Revision Control:

Version 1.0 *11 January 2022*	Original Release
Version 2.0 *08 February 2022*	Remediation available for *M241/M251*. Added *Easy Harmony ET6 (HMIET Series) and Easy Harmony GXU (HMIGXU Series)* to the list of affected products.
Version 3.0 *12 April 2022*	Remediation available for *Eurotherm E+PLC400* and *Eurotherm E+PLC tools*. End of commercialization for *Eurotherm E+PLC100*.
Version 4.0 *12 July 2022*	Remediation available for *EcoStruxure™ Machine Expert.*
Version 5.0 *10 January 2023*	A remediation is available for Harmony/Magelis HMI products (page 3).
Version 6.0 *14 March 2023*	A remediation is available for HMISTU Series / HMIGTO Series / HMIGTU Series / HMIGTUX Series / HMIGK Series (page 4).
Version 7.0 *11 April 2023*	Remediation available for Easy Harmony ET6 (HMIET Series) and Easy Harmony GXU (HMIGXU Series) (page 4).

Product Security Office

Digitally signed by Product Security Office
Date: 2023.04.10 12:29:06 -04'00'