# Schneider Electric Security Notification

## CODESYS V3 Runtime, Development System and Gateway Vulnerabilities

**11 January 2022**

## 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.

## 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 Mitigations

Schneider Electric is establishing a remediation plan 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 exploit

| Affected Product & Versions | CVEs | Temp Mitigations |
|---|---|---|
| M241/M251<br>*All Versions* | CVE-2021-29241<br>CVE-2021-33485 | Schneider Electric is establishing a remediation plan 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 recommended mitigations provided below to reduce the risk of exploit. |
| EcoStruxure Machine Expert<br>*All Versions* | CVE-2021-21863<br>CVE-2021-21864<br>CVE-2021-21865<br>CVE-2021-21866<br>CVE-2021-21867<br>CVE-2021-21868<br>CVE-2021-21869 | Schneider Electric is establishing a remediation plan 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 recommended mitigations provided below to reduce the risk of exploit. |
| Harmony/ Magelis<br>HMISTU Series<br>HMIGTO Series<br>HMIGTU Series<br>HMIGTUX Series<br>HMIGK Series<br>HMISCU Series<br><br>*Vijeo Designer V6.2 SP11 Hotfix 3 and prior* | CVE-2021-29241 | Schneider Electric is establishing a remediation plan 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 recommended mitigations provided below to reduce the risk of exploit. |

| | | |
|---|---|---|
| Eurotherm E+PLC100 *All Versions* | CVE-2021-33485 | Schneider Electric is establishing a remediation plan 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 recommended mitigations provided below to reduce the risk of exploit. |
| Eurotherm E+PLC400 *All Versions* | CVE-2021-33485 | Schneider Electric is establishing a remediation plan 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 recommended mitigations provided below to reduce the risk of exploit. |
| Eurotherm E+PLC tools *All Versions* | CVE-2021-29240<br>CVE-2021-29241<br>CVE-2021-21863<br>CVE-2021-21864<br>CVE-2021-21865<br>CVE-2021-21866<br>CVE-2021-21867<br>CVE-2021-21868<br>CVE-2021-21869 | Schneider Electric is establishing a remediation plan 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 recommended mitigations provided below to reduce the risk of exploit. |

## 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.

## 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

# Schneider Electric Security Notification

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**<br>*11 January 2022* | Original Release |

Product Security Office

Digitally signed by Product Security Office
Date: 2022.01.08 20:03:50 -05'00'