

## Schneider Electric Security Notification

# PLC Simulator on EcoStruxure™ Control Expert and Process Expert

10 November 2020 (14 February 2023)

## Overview

Schneider Electric is aware of multiple vulnerabilities in its PLC Simulator for EcoStruxure™ Control Expert product.

PLC Simulator feature is part of the [Ecostruxure™ Control Expert](#) and [Ecostruxure™ Process Expert](#) software and it helps users to review and test their configurations files in a simulation environment; it is not intended to be used as a controller CPU in a production environment.

Failure to apply the mitigations provided below may risk unauthorized command execution or denial of service, which could result in undesired actions by the PLC simulator software.

**February 2023 Update:** There was an update to the PLC Simulator user manual to reflect the mitigation below ([page 3](#)).

## Affected Products and Versions

- PLC Simulator for EcoStruxure™ Control Expert prior to v15.0 SP1
- PLC Simulator for Unity Pro (former name of EcoStruxure™ Control Expert), all versions
- PLC Simulator for EcoStruxure™ Process Expert, all versions

## Vulnerability Details

CVE ID: **CVE-2020-7559**

CVSS v3.0 Base Score 10.0 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

A *CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')* vulnerability exists that could cause a crash of the PLC simulator present in EcoStruxure™ Control Expert software and EcoStruxure™ Process Expert when receiving a specially crafted request over Modbus.

CVE ID: **CVE-2020-7538**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A *CWE-754: Improper Check for Unusual or Exceptional Conditions* vulnerability exists that could cause a crash of the PLC simulator present in EcoStruxure™ Control Expert software and EcoStruxure™ Process Expert when receiving a specially crafted request over Modbus.

## Schneider Electric Security Notification

CVE ID: **CVE-2020-28211**

CVSS v3.0 Base Score 7.4 | High | CVSS:3.0/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:N

A *CWE-863: Incorrect Authorization* vulnerability exists that could cause bypass of authentication when overwriting memory using a debugger.

CVE ID: **CVE-2020-28212**

CVSS v3.0 Base Score 9.1 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H

A *CWE-307: Improper Restriction of Excessive Authentication Attempts* vulnerability exists that could cause unauthorized command execution when a brute force attack is done over Modbus.

CVE ID: **CVE-2020-28213**

CVSS v3.0 Base Score 8.1 | High | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

A *CWE-494: Download of Code Without Integrity Check* vulnerability exists that could cause unauthorized command execution when sending specially crafted requests over Modbus.

### Remediation

EcoStruxure™ Control Expert Version 15.0 SP1 product includes a fix for the vulnerability CVE-2020-7559 and is available for download here:

[https://www.se.com/ww/en/download/document/EcoStruxureControlExpert\\_15SP1](https://www.se.com/ww/en/download/document/EcoStruxureControlExpert_15SP1)

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 follow the recommendations in the Mitigation section below to reduce the risk of exploit.

### Mitigation

Customers should immediately apply the following mitigations to reduce the risk of exploit of the CVE-2020-7538, CVE-2020-28211, CVE-2020-28212, CVE-2020-28213

- **V15.0 of the EcoStruxure™ Control Expert software** includes a mitigation for these vulnerabilities, when applied with the steps outlined below, and is available for download here:

## Schneider Electric Security Notification

<https://www.se.com/ww/en/product-range-download/548-ecostruxure%E2%84%A2-control-expert/?parent-subcategory-id=3950&filter=business-1-industrial-automation-and-control&selected-node-id=12365959203#/software-firmware-tab>

- **EcoStruxure™ Process Expert 2020 R2 software**, includes a mitigation, when applied with the steps outlined below, for these vulnerabilities and is available for download on the EcoStruxure Process Expert Support Portal (registration is needed): <https://app.schneider-electric.com/ecostruxure-hybrid-dcs/>

After downloading the updated software listed above, the following steps are required to mitigate the vulnerability:

1. Harden the Engineering Workstation running PLC Simulator
  - Follow workstation, network and site-hardening guidelines in the Recommended Cybersecurity Best Practices guide available for download [here](#).
2. On **V15.0 of the EcoStruxure™ Control Expert** and **EcoStruxure™ Process Expert 2020 R2 software**, in the option dialog box of the PLC simulator, customers are requested to set the Listening IP Address to:
  - a. 127.0.0.1 (localhost), which will prevent remote network connections to the PLC simulator; **or**
  - b. When deployed as a remote access system the IP Address should be configured to be the same as the system that will be running the PLC simulator.

**Note:** Customers are informed that on EcoStruxure™ Control Expert v15.0 and EcoStruxure™ Process Expert 2020 R2 software and prior, the default listening IP address is: 0.0.0.0. The default setting exposes the PLC simulator to the vulnerabilities described in this bulletin. The default listening IP address is configurable from v15.0 and 2020 R2 and above.

**Update:** Starting with EcoStruxure™ Control Expert v15.0 SP1 and above the default listening IP address is: 127.0.0.1. **The same setting is also recommended for the PLC Simulator and is documented in the PLC Simulator user manual available [here](#)**

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 mitigations provided above or in case of older versions of EcoStruxure™ Control Expert software, they should immediately apply the following mitigations to reduce the risk of exploit:

1. Setup network segmentation and implement a firewall to block all unauthorized access to port 502/TCP

## Schneider Electric Security Notification

2. Harden the Engineering Workstation running PLC Simulator for EcoStruxure™ Control Expert and EcoStruxure™ Process Expert
  - Follow workstation, network and site-hardening guidelines in the Recommended Cybersecurity Best Practices guide available for download [here](#).

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 for the devices that it is intended for.
- 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 researchers for identifying and helping to coordinate a response to these vulnerabilities:

CVE	Researcher
CVE-2020-7559	Alexander Perez-Palma and Jared Rittle (Cisco Talos)

## Schneider Electric Security Notification

CVE-2020-7538	Parity Dynamics Research Team
CVE-2020-28211, CVE-2020-28212, CVE-2020-28213	Flavian Dola (Airbus Cybersecurity)

### 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. These organizations will be fully aware of this situation and can support you through the process.

<https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp>

<https://www.se.com/ww/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.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.

## Schneider Electric Security Notification

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](http://www.se.com)

Revision Control:

<b>Version 1.0</b> <i>10 November 2020</i>	<b>Original Release</b>
<b>Version 2.0</b> <i>09 March 2021</i>	Future remediation plan will include a fix for CVE-2020-7559 (page 2)
<b>Version 3.0</b> <i>08 June 2021</i>	PLC Simulator for Ecostruxure™ Process Expert has been added as an affected product. In addition, a new mitigation option has been added. (page 1-3)
<b>Version 3.1</b> <i>13 July 2021</i>	Added fix of CVE-2020-7559 for PLC Simulator for EcoStruxure™ Control Expert
<b>Version 4.0</b> <i>14 February 2023</i>	There was an update to the PLC Simulator user manual to reflect the mitigation below ( <a href="#">page 3</a> ).