Schneider Electric Security Notification

PLC Simulator on EcoStruxure™ Control Expert and Process Expert (V3.1)

10 November 2020 (13 July 2021)

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.

July 2021 update: A fix for CVE-2020-7559 is available in EcoStruxure™ Control Expert v15.0 SP1

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.

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

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:

  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.

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
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.

Schneider Electric Security Notification

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)
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

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

Schneider Electric Security Notification

Revision Control:

Version 1.0 *10 November 2020*	Original Release
Version 2.0 *9 March 2021*	Future remediation plan will include a fix for CVE-2020-7559 (page 2)
Version 3.0 *08 June 2021*	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)
Version 3.1 *13 July 2021*	Added fix of CVE-2020-7559 for PLC Simulator for EcoStruxure™ Control Expert (page 2)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.07.11 22:11:29 -04'00'