# Schneider Electric Security Notification

## EcoStruxure$^{TM}$ Control Expert, EcoStruxure$^{TM}$ Process Expert, SCADAPack RemoteConnect™ for x70

**14 September 2021 (12 July 2022)**

## Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Control Expert, EcoStruxure™ Process Expert, SCADAPack RemoteConnect™ for x70 software products. This vulnerability lays in the functions used to handle project files.

The EcoStruxure™ Control Expert product is a software to design, diagnose, maintain and update applications for Modicon M340, M580 and M580 Safety, Momentum, and legacy Premium and Quantum PLCs.

The EcoStruxure™ Process Expert DCS is a single automation system to engineer, operate, and maintain your entire infrastructure for a sustainable, productive and market-agile plant.

The SCADAPack RemoteConnect™ for x70 product is a Windows-based application based on EcoStruxure™ Control Expert software components that provides a programming and configuration environment for the SCADAPack x70 RTU series, which is comprised of the SCADAPack 470, 474, 570, 574 and 575 Smart RTUs.

Failure to apply the mitigations provided below may result in an authenticated user opening a corrupted project file, which could then result in arbitrary code execution on the engineering workstation.

July 2022 Update: A release is available for SCADAPack RemoteConnect™ R2.7.3 that addresses this vulnerability.

## Affected Products and Versions

| Product | Version |
|---|---|
| EcoStruxure™ Control Expert | V15.0 SP1 and prior (including former Unity Pro) |
| EcoStruxure™ Process Expert | 2020 and prior (including former HDCS) |
| SCADAPack RemoteConnect™ for x70 | All versions prior to R2.7.3 |

## Vulnerability Details

CVE ID: **CVE-2021-22797**

CVSS v3.1 Base Score 7.8 | High | CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

A *CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal)* vulnerability exists that could cause malicious script to be deployed in an unauthorized location and may result in code execution on the engineering workstation when a malicious project file is loaded in the engineering software.

## Remediations

| Affected Product & Version | Remediations and Mitigations |
|---|---|
| EcoStruxure™ Control Expert<br>*V15.0 SP1 and prior (including former Unity Pro)* | V15.1 and prior of EcoStruxure™ Control Expert includes a fix for these vulnerabilities and is available for download here:<br>https://www.se.com/ww/en/download/document/EcoStruxureControlExpert_V15.1/ |
| EcoStruxure™ Process Expert<br>*2020 and prior (including former HDCS)* | V2021 and prior of EcoStruxure™ Process Expert includes a fix for these vulnerabilities and is available for download here:<br>https://www.se.com/myschneider/documentsDownloadCenterDetail/in/en/EPE2021Release<br>It is recommended to first read the ReadMe in its entirety before proceeding with the software installation. |
| SCADAPack RemoteConnect™ for x70<br>*All versions prior to version R2.7.3* | Version *R2.7.3* and prior of *SCADAPack RemoteConnect* includes a fix for this vulnerability and is available for download here:<br>RemoteConnect for the SCADAPack x70 \| Schneider Electric Exchange Marketplace (se.com)<br>Note: Users no longer need to update the RemoteConnect application when there is a Control Expert update<br>If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:<br>• Store project files in a secure storage and limit access to the files. Restrict the access to the files to only trusted users<br>• When exchanging the files over the network, use secure communication protocols<br>• Harden your workstation running SCADAPack RemoteConnect™ for the 70x<br>• Compute a checksum on your project files and check the consistency of this checksum to verify the integrity before usage<br>• Start the software without administrator rights, to prevent from copying extracted files in critical system folders |

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

## 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 researcher for identifying and helping to coordinate a response to this vulnerability:

| CVE | Researcher |
|---|---|
| CVE-2021-22797 | Kimiya working with Trend Micro Zero’s Day Initiative |

## 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

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**<br>*14 September 2021* | Original Release |
| **Version 2.0**<br>*08 March 2022* | EcoStruxure™ Control Expert V15.1 and EcoStruxure™ Process Expert 2021 include a fix for these vulnerabilities |
| **Version 3.0**<br>*12 July 2022* | A release is available for SCADAPack RemoteConnect™ R2.7.3 that addresses this vulnerability. |

Product Security Office Digitally signed by Product Security Office
Date: 2022.07.07 12:36:55 -04'00'