Schneider Electric Security Notification

EcoStruxure™ Control Expert, EcoStruxure™ Process Expert, SCADAPack RemoteConnect™ for x70

14 September 2021

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.

Affected Products and Versions

- EcoStruxure Control Expert, all versions (including former Unity Pro)
- EcoStruxure Process Expert, all versions (including former HDCS)
- SCADAPack RemoteConnect for x70, all versions

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.

Mitigations

Schneider Electric is establishing a remediation plan for future versions of the affected products that will include a fix for this vulnerability. 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:

- Store project files in a secure storage and limit access to the files. Restrict the access to the files to only trusted users
- When exchanging the files over the network, use secure communication protocols
- Harden your workstation running EcoStruxure Control Expert or EcoStruxure Process Expert, or SCADAPack RemoteConnect™.
- Compute a checksum on your project files and check the consistency of this checksum to verify the integrity before usage
- Start the software without administrator rights, to prevent from copying extracted files in critical system folders

Customers still using Unity Pro should strongly consider migrating to EcoStruxure Control Expert as this is where this issue will be fixed. Please contact your local Schneider Electric technical support for more information.

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 researcherfor 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

Schneider Electric Security Notification

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 *14 September 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.09.11 08:58:29 -04'00'