Schneider Electric Security Notification

EcoStruxure™ Control Expert, EcoStruxure™ Process Expert and RemoteConnect™ (V2.0)

8 December 2020 (13 July 2021)

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Control Expert product and EcoStruxure™ Process Expert.

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

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

The RemoteConnect™ product is a Windows-based application based on EcoStruxure™ Control Expert (Unity Pro) 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 risk opening a malicious file, which could result in crash of the software or unexpected code execution.

July 2021 update: Added availability of fix in the version 15.0 SP1 of EcoStruxure Control Expert and added EcoStruxure™ Process Expert and RemoteConnect™ as impacted products.

Affected Products and Versions

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

Vulnerability Details

CVE ID: **CVE-2020-7560**

CVSS v3.0 Base Score 8.6 | High | CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

A CWE-123 - Write-what-where Condition vulnerability exists that could cause a crash of the software or unexpected code execution when opening a malicious file in the engineering software.

Remediation

EcoStruxure Control Expert v15.0 SP1 product includes a fix for this vulnerability and is available for download here:

https://www.se.com/ww/en/download/document/EcoStruxureControlExpert_15SP1

Important Note:

- The fix is provided through the additional feature “file encryption”, for further information on the feature and how to set it up please refers to the chapter “file encryption” of the help file available in the EcoStruxure Control Expert v15.0 SP1.
- This feature is proposed by default when creating a new project.
- This feature is also available, after selecting “project” in structural view, in the “Edit/ Properties/ Project & Controller Protection” menu.
- **For new projects:**
  - Customers are recommended to apply this feature to all new projects.
- **For existing projects:**
  - Customers are recommended to apply this feature to the existing projects coming from trusted source. For .sta project files, as a reminder, project modification can be done in connected mode to prevent desynchronization and keep the controller in RUN state.
- It is possible to set a security level specific to the Derived Function Blocks (DFB) in addition to the file encryption feature. Please refer to the chapter "How to protect a DFB type" in the EcoStruxure Control Expert help file for further information.
- Customers are recommended to share project files only when configured with the encryption feature described above.

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 apply the following mitigations to reduce the risk of exploit.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

- Store the project files in a secure storage and restrict the access to only trusted users
- When exchanging files over the network, use secure communication protocols
- Encrypt project files when stored
- Only open project files received from trusted source

- Compute a hash of the project files and regularly check the consistency of this hash to verify the integrity before usage
- Harden the workstation running EcoStruxure Control Expert or Unity Pro

Mitigations

Schneider Electric is establishing a remediation plan for the future product versions of **EcoStruxure™ Process Expert** and **RemoteConnect™** that will include a fix for the above vulnerability.

We will update this document when the remediation is available. Until then, customers should immediately apply the following mitigations to reduce the risk of exploit:

- Store the project files in a secure storage and restrict the access to only trusted users
- When exchanging files over the network, use secure communication protocols
- Encrypt project files when stored
- Only open project files received from trusted source
- Compute a hash of the project files and regularly check the consistency of this hash to verify the integrity before usage
- Harden the workstation running EcoStruxure™ Control Expert, EcoStruxure™ Process Expert or RemoteConnect™

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Ensure the cybersecurity features in Schneider Electric solutions are always enabled.
- 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 when applicable do not leave them in the “Program” mode.
- Never connect programming software and engineering workstations to any network other than the network that it is intended.
- ICS networks should be appropriately partitioned, and not directly connected to business networks or the Internet.
- 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.
- Customers are encouraged to implement best practices covered in the Top 20 Secure PLC Coding Practices to help improve the security posture of their Industrial Control Systems.

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-2020-7560	Jared Rittle (Cisco Talos)

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

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 *8 December 2020*	Original Release
Version 2.0 *12 July 2021*	Added fix availability on Ecostruxure Control Expert v15.0 SP1 and added EcoStruxure™ Process Expert and RemoteConnect as impacted product. (pages 1-3)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.07.11 15:54:27 -04'00'