Schneider Electric Security Notification

AT&T Labs Compressor (XMill) and Decompressor (XDemill) used by EcoStruxure^{TM} Control Expert, EcoStruxure^{TM} Process Expert and SCADAPack RemoteConnect™ for x70

10 August 2021 (12 July 2022)

Overview

Schneider Electric is aware of multiple vulnerabilities on AT&T Labs' Compressor (XMill) and decompressor (XDemill) third party components used by EcoStruxure Control Expert, EcoStruxure Process Expert and SCADAPack RemoteConnect™ for x70.

Failure to apply the mitigations provided below may lead to the execution of a malicious file, which could result in code execution with elevated privileges on the engineering workstation. For an attack to be successful, an attacker requires access to the engineering workstation and then needs to trick a valid user to run a script or load a malicious project file.

July 2022 Update: A release is available for SCADAPack RemoteConnect™ R2.7.3 that addresses workstation vulnerabilities related to the issues listed below.

Affected Products and Versions

Product	Version
EcoStruxure™ Control Expert	All versions (including former Unity Pro) prior to V15.1 HF001
EcoStruxure™ Process Expert	All versions (including former HDCS) prior to V2021
SCADAPack RemoteConnect™ for x70	All versions prior to R2.7.3

Vulnerability Details

The vulnerabilities reported on XDemill and XMill are triggered through the execution of a malicious script on the engineering workstation, or when loading a specially crafted project file into the engineering tool. The successful exploitation of these vulnerabilities may lead to code execution with elevated privileges on the engineering workstation.

The following CVEs have been reserved by external organizations. Additional vulnerability details can be found at the links below:

- CVE-2021-21810
- CVE-2021-21811
- CVE-2021-21812
- CVE-2021-21813
- CVE-2021-21814
- CVE-2021-21815
- CVE-2022-26507
- CVE-2021-21825
- CVE-2021-21826
- CVE-2021-21827
- CVE-2021-21828
- CVE-2021-21829
- CVE-2021-21830

Remediation

Affected Product & Version	Remediation
EcoStruxure™ Control Expert *All versions (including former Unity Pro) prior to v15.1 HF001*	V15.1 HF001 of EcoStruxure™ Control Expert includes a fix for these vulnerabilities and is available for download here: https://www.se.com/ww/en/download/document/ControlExpert_V151_HF001/ 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 channels • Only open project files received from a 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 • Customers using Unity Pro should strongly consider migrating to EcoStruxure Control Expert.
EcoStruxure™ Process Expert *All versions (including former HDCS) prior to v2021*	V2021 of EcoStruxure™ Process Expert includes a fix for these vulnerabilities and is available for download here: https://www.se.com/myschneider/documentsDownloadCenterDetail/in/en/EPE2021Release It is recommended to first read the ReadMe first document before proceeding with the software installation. 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 channels • Only open project files received from a 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 Process Expert

SCADAPack RemoteConnect™ for x70 *All versions prior to R2.7.3*	Version R2.7.3 of SCADAPack RemoteConnect™ includes a fix for these vulnerabilities and is available for download here at the Schneider Electric Exchange: https://shop.exchange.se.com/en-US/apps/58663 Note: Users no longer need to update the RemoteConnect™ application when there is a Control Expert update. 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 channels • Only open project files received from a 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 SCADAPack RemoteConnect™ for x70

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.

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	Researchers
CVE-2021-21810, CVE-2021-21825, CVE-2021-21811 CVE-2021-21826, CVE-2021-21812, CVE-2021-21827 CVE-2021-21813, CVE-2021-21828, CVE-2021-21814 CVE-2021-21829, CVE-2021-21815, CVE-2021-21830	Carl Hurd (Cisco Talos)
CVE-2022-26507	Uri Katz of Claroty Research

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 *10 August 2021*	Original Release
Version 2.0 *08 March 2022*	Remediation update
Version 2.1 *09 March 2022*	Recently released versions of EcoStruxure™ Control Expert and EcoStruxure™ Process Expert previously communicated to address these vulnerabilities were found to not fully address the issues as stated in a previous update of this notification. Customers are encouraged to follow the mitigations provided below.
Version 3.0 *12 April 2022*	Added remediation for EcoStruxure™ Control Expert V15.1 HF001 and EcoStruxure™ Process Expert V2021. Schneider Electric is establishing a remediation plan for future versions of SCADAPack RemoteConnect for x70. Added CVE-2022-26507.
Version 4.0 *12 July 2022*	Added remediation for SCADAPack RemoteConnect™ for x70.

Product Security Office Digitally signed by Product Security Office
Date: 2022.07.07 12:37:30 -04'00'