Schneider Electric Security Notification

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

10 August 2021

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.

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

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 an external organization. Additional vulnerability details can be found at https://talosintelligence.com/vulnerability_reports.

https://talosintelligence.com/vulnerability_reports/TALOS-2021-1292

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

Schneider Electric Security Notification

Mitigations

Schneider Electric encourages all industrial companies to ensure they have implemented cybersecurity best practices across their operations and supply chains to reduce cyber risks. Where appropriate this includes locating industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; preventing mission critical systems and devices from being accessed from outside networks; systematically applying security patches.

Schneider Electric is establishing a remediation plan for the future versions of EcoStruxure Control Expert, EcoStruxure Process Expert, and SCADAPack RemoteConnect for x70 that will include a fix for these vulnerabilities. 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

For EcoStruxure Control Expert all versions (including former Unity Pro):

- Download and setup EcoStruxure Control Expert V15.0 SP1 from this link https //www.se.com/ww/en/download/document/EcoStruxureControlExpert_15SP1
    - Use the new “file encryption” feature available on EcoStruxure Control Expert V15.0 SP1 in order to protect the project files.
- Store the project files in a secure storage and restrict the access to only trusted users
- Carefully check scripts containing **xmill.exe** and **xdmill.exe** when coming from an untrusted source
- 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, EcoStruxure Process Expert and SCADAPack RemoteConnect™ for x70
- Customers using Unity Pro should strongly consider migrating to EcoStruxure Control Expert.

For EcoStruxure Process Expert, all versions (including former HDCS) and SCADAPack RemoteConnect for x70:

- Store the project files in a secure storage and restrict the access to only trusted users
- Carefully check scripts containing **xmill.exe** and **xdmill.exe** when coming from an untrusted source
- 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, EcoStruxure Process Expert and SCADAPack RemoteConnect™ for x70
- Customers using Unity Pro should strongly consider migrating to EcoStruxure Control Expert.

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 Carl Hurd (Cisco Talos) for identifying and helping to coordinate a response to these vulnerabilities.

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.

Schneider Electric Security Notification

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

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 *10 August 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.08.07 21:33:24 -04'00'