TLP:WHITE



# ICS Advisory (ICSA-21-259-02)

## Schneider Electric EcoStruxure and SCADAPack

Original release date: September 16, 2021

## Legal Notice



## 1. EXECUTIVE SUMMARY

- CVSS v3 7.8
- ATTENTION: Low attack complexity
- Vendor: Schneider Electric
- Equipment: EcoStruxure Control Expert, EcoStruxure Process Expert, SCADAPack RemoteConnect for x70
- Vulnerability: Path Traversal

## 2. RISK EVALUATION

Successful exploitation of this vulnerability could result in code execution on the engineering workstation.

## 3. TECHNICAL DETAILS

## 3.1 AFFECTED PRODUCTS

The following products and versions are affected:

- EcoStruxure Control Expert: All versions, including former Unity Pro
- EcoStruxure Process Expert: All versions, including former HDCS
- SCADAPack RemoteConnect for x70: All versions

## 3.2 VULNERABILITY OVERVIEW

### 3.2.1 IMPROPER LIMITATION OF A PATHNAME TO A RESTRICTED DIRECTORY ('PATH TRAVERSAL') CWE-22

When a malicious project file is loaded on the engineering workstation software, it deploys a malicious script to execute arbitrary code in unauthorized locations.

CVE-2021-22796 has been assigned to this vulnerability. A CVSS v3 base score of 7.8 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).

## 3.3 BACKGROUND

- CRITICAL INFRASTRUCTURE SECTORS: Commercial Facilities, Energy, Food and Agriculture, Government Facilities, Transportation Systems, Water and Wastewater Systems
- COUNTRIES/AREAS DEPLOYED: Worldwide
- COMPANY HEADQUARTERS LOCATION: France

## 3.4 RESEARCHER

kimiya, working with Trend Micro Zero’s Day Initiative, reported this vulnerability to CISA.

## 4. MITIGATIONS

Schneider Electric is establishing a remediation plan for future versions of the affected products that will include a fix for this vulnerability. CISA will update this document when the remediations are available.

Schneider Electric recommends users immediately apply the following mitigations to reduce the risk of exploitation:

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

Users still using Unity Pro should strongly consider migrating to EcoStruxure Control Expert. Please contact the local Schneider Electric technical support for more information.

To stay informed of all updates, including details on affected products and remediation plans, subscribe to Schneider Electric's security notification service.

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize VPN is only as secure as its connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices on the ICS webpage on us-cert.cisa.gov. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.cisa.gov in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to CISA for tracking and correlation against other incidents.

CISA also recommends users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open unsolicited attachments in email messages.
- Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.
- Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

No known public exploits specifically target this vulnerability. This vulnerability is not exploitable remotely.

## Contact Information

For any questions related to this report, please contact the CISA at:

Email: CISAservicedesk@cisa.dhs.gov
Toll Free: 1-888-282-0870

For industrial control systems cybersecurity information: https://us-cert.cisa.gov/ics
or incident reporting: https://us-cert.cisa.gov/report

CISA continuously strives to improve its products and services. You can help by choosing one of the links below to provide feedback about this product.

---