Life Is On Schneider Electric

Schneider Electric Security Bulletin

EcoStruxure™ Operator Terminal Expert

28 January 2020

Overview

Schneider Electric will always be as open, transparent and collaborative as possible to help our customers secure and protect their people, assets and operations from cyber risk.

As part of this ongoing commitment, we participated in the Pwn2Own event at the S4 Conference from January 21-23, 2020. Through it, we identified several vulnerabilities in our EcoStruxure Operator Terminal Expert, a human machine interface (HMI) configuration software, used to monitor and operate connected controllers in an industrial environment.

Our cybersecurity teams are working diligently to investigate these vulnerabilities, in collaboration with conference organizers and independent researchers. We will announce remediations and mitigations as soon as they are available. Until then, our customers should immediately ensure they have implemented cybersecurity best practices across their operations to protect themselves. Where appropriate this includes locating industrial systems and remotely accessible devices behind firewalls; installing physical controls to prevent unauthorized access; and preventing mission-critical systems and devices from being accessed from outside networks.

Defending against newer, more innovative and increasingly dangerous cyber threats can't be limited to a single company, industry or region – it must be a global effort. Events like Pwn2Own are a critical part of Schneider Electric's commitment to continually improving our customers' ability to detect, mitigate and prevent cybersecurity risks.

Details

During the Pwn2Own event, researchers identified two issues in EcoStruxure™ Operator Terminal Expert software:

- An arbitrary DLL loading issue,
- A traversal path issue in the software.

These two vulnerabilities could lead to malicious code execution on workstations running EcoStruxure™ Operator Terminal Expert software.

Recommended Mitigations

Customers are requested to apply immediately the following mitigations to reduce risks:

- Harden your workstation following the best cybersecurity practices (antivirus, updated operating systems, strong password policies, Application White Listing software, etc.) using the following guideline: https://www.se.com/us/en/download/document/CS-Best-Practices-2019-340/
- Do not execute EcoStruxure™ Operator Terminal Expert software with Windows administrator privileges.
- Protect your workstation with a firewall and make sure it is used on a trusted network.
- Install the HMI product on a secure network.
- Use EcoStruxure™ Operator Terminal Expert software only on a trusted workstation.
- Only accept project files from trusted users.
- Only simulate/transfer trusted applications to the HMI.
- Manage your project files and exported files securely to avoid information disclosure or unexpected modifications of the data.
- Define a strong password in your project. Enable “use complex password” function in the section “Security / Settings / use complex password” to improve the protection of your project.

General Security Recommendations

Our customers should always ensure they are following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person has access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for which it is intended.
- All methods of mobile data exchange with the isolated network, such as via CDs, USB drives, etc., should be scanned before use in the terminals or before any node is connected to these networks.
- Laptops that are connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or systems, and ensure they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

Schneider Electric Security Bulletin

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate them. For more details and assistance on how to protect your installation, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **make the most of their energy and resources**, 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 about our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1 *28 January 2020*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2020.01.27 12:02:34 -05'00'