Schneider Electric Security Bulletin

APT Cyber Tools Targeting ICS/SCADA Devices

13 April 2022 (14-Apr-22)

Overview

Schneider Electric, working in close collaboration with the United States Department of Energy, Homeland Security, and cybersecurity defense partner, Mandiant, identified and developed protective measures to defend against an APT (Advanced Persistent Threat) Cyberattack Tools/Framework still in development that would target a set of our Programmable Logic Controllers (PLCs). The following analysis and protective measures come from this public-private partnership collaboration. In addition, this Security Bulletin includes a range of technical analytics, hunting tools, and specific mitigations to help asset owners find and defend against the framework.

The collaboration between private-sector cyber experts (Mandiant) and the affected Original Equipment Manufacturer (Schneider Electric) and Government agencies led to higher-confidence mitigations for protecting stakeholders. This is an instance of successful collaboration to deter threats on critical infrastructure before they occur and further underscores how public-private partnerships are instrumental in detecting and countering threats before they can be deployed proactively.

Schneider Electric is committed to working together with Governments and Partners to advance our shared goal of protecting our customers, communities, and the environment from all serious cybersecurity threats.

Details

In early 2022, Mandiant, in partnership with Schneider Electric, analyzed a set of novel industrial control system (ICS)-oriented attack tools—which they call INCONTROLLER, and also tracked as PIPEDREAM by Dragos—built to target machine automation devices. The framework can interact with specific industrial equipment embedded in different types of machinery leveraged across multiple industries.

While we are not aware, at the date of this publication, of any confirmed or potential targets leveraging INCONTROLLER, the framework poses a critical risk to organizations using the targeted devices. The framework has capabilities related to disruption, sabotage, and potentially physical destruction.

If the framework is used against one of the targeted devices, it would allow for use of the same standard features as the programming tool or Modbus client or OPC-UA client. Any action that can be performed by an attacker using a legitimate programming tool or modbus client can likewise be performed using the framework. Other than that, we have not identified any weakness or vulnerability being exploited. Depending on the features utilized in the framework and the security features configured on the device, an attacker can perform actions such as:

- Perform a network scan to discover the device
- Change the IP address to communicate with the framework or make the device unreachable

- Send Modbus frame (standard or proprietary)
- Automate connection to PLC in order to bruteforce the password using standard programming protocols
- Upload and download files (configuration, firmware, application, recipes, etc)
- Execute denial of service attacks to force the user to authenticate again or make the device unreachable
- Perform read/write to OPC-UA server

Potentially Targeted Products

The investigated version of the framework contains information that indicates the potential to impact the following Schneider Electric devices:

Product	Versions
TM221	All
TM241/TM251	All
TM258/LMC058	All
LMC078	All
TM238	All
PacDrive LMC	All

The framework has the ability to communicate with all versions of Modbus and CODESYS devices. This includes devices managed by EcoStruxure Machine Expert software and SoMachine software. Microgrid Operation (EMO-M) could also be potentially targeted, as the programming tool for TM251 (PLC of EMO-M solution) is EcoStruxure Machine Expert (ESME) and the core of ESME is CODESYS.

Recommended Mitigations

Customers should immediately implement the following recommendations to protect their Schneider Electric devices:

- Update EcoStruxure Machine Expert and EcoStruxure Machine Expert Basic to the latest versions using Schneider Electric Software Update software or with following links:
  - EcoStruxure Machine Expert
  - EcoStruxure Machine Expert-Basic
- Update firmware of your programmable logic controllers:
  - Using Controller Assistant for Machine Expert devices
  - Using Controller Update feature in Commissioning tab of EcoStruxure Machine Expert Basic
- For TM221, set up a strong password for read/write of application in the “Application Protection page
- For Machine Expert programmable logic controllers, replace default account with your own and set up a strong password
- Disable unused protocol in the device’s Ethernet pages, especially:

  - (Auto) Discovery protocol (UDP ports 27126, 27127 and 3702)
  - Programing protocol (TCP port 502 for TM221)
  - Machine Expert protocol (UDP ports 1740 to 1743, TCP ports 1105 and 11740)
  - Modbus protocol (TCP port 502)
- Check that the application on the device has not been modified.

Additionally, the Cybersecurity Guidelines for EcoStruxure Machine Expert, Modicon and PacDrive Controllers and Associated Equipment User Guide should be used to harden your Schneider Electric product.

You should pay special attention to features and cybersecurity devices that help to restrict access to authorized users only. Some examples are the Intrusion Detection System, network firewalls, secure remote access, device authentication, device firewall, disabling/filtering unsecure or programming protocols.

We recommend our customers to check the TTP section on the CISA advisory to map to the MITRE ATT&CK for ICS framework.

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.
- Have a recovery strategy; test your backups frequently.
- Employ Defense in Depth strategy to protect your environment and assets.
- Never connect programming software to any network other than the network intended for that device.
- 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.

Additional Resources

For further information related to the framework, visit:

- CISA Advisory (AA22-103A)
- Mandiant publication
- CODESYS Advisory 2022-08

For More Information

This document provides an overview of the identified risks 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

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.

Schneider Electric Security Bulletin

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 *13 April 2022*	Original Release
Version 1.1 *14 April 2022*	Added link to the CODESYS Advisory 2022-08 (page 4)

Product Security Office

Digitally signed by Product Security Office
Date: 2022.04.20 11:03:42 -07'00'