Schneider Electric Security Notification

Wibu-Systems CodeMeter Vulnerabilities

13 October 2020

Overview

Schneider Electric is aware of multiple vulnerabilities disclosed by Wibu-Systems in the CodeMeter licensing manager product which is used by some Schneider Electric and Eurotherm offers.

Failure to apply the mitigations provided below may risk various types of attack on CodeMeter, which could allow an attacker to alter and forge a license file, cause a denial-of-service condition, potentially attain remote code execution, read heap data, and prevent normal operation of third-party software dependent on the CodeMeter.

Affected Product and Version

Affected Products	Versions
EcoStruxure Machine Expert (formerly known as SoMachine and SoMachine Motion)	All versions
E+PLC400	All versions
E+PLC100	All versions
E+PLC_Setup	All versions
EcoStruxure Machine SCADA Expert	All versions

Vulnerability Details

CVE ID: **CVE-2020-14509**

CVSS v3.0 Base Score 10.0 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Multiple memory corruption vulnerabilities exist where the packet parser mechanism of CodeMeter (All versions prior to 7.10a) does not verify length fields. An attacker could send specially crafted packets to exploit these vulnerabilities.

CVE ID: **CVE-2020-14513**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CodeMeter (All versions prior to 6.81) and the software using it may crash while processing a specifically crafted license file due to unverified length fields.

CVE ID: **CVE-2020-14515**

CVSS v3.0 Base Score 7.4 | High | CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:H

CodeMeter (All versions prior to 6.90 when using CmActLicense update files with CmActLicense Firm Code) has an issue in the license-file signature checking mechanism, which allows attackers to build arbitrary license files, including forging a valid license file as if it were a valid license file of an existing vendor. Only CmActLicense update files with CmActLicense Firm Code are affected.

CVE ID: **CVE-2020-14517**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/ AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Protocol encryption can be easily broken for CodeMeter (All versions prior to 6.90 are affected, including Version 6.90 or newer only if CodeMeter Runtime is running as server) and the server accepts external connections, which may allow an attacker to remotely communicate with the CodeMeter API.

CVE ID: **CVE-2020-14519**

CVSS v3.0 Base Score 8.1 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

This vulnerability allows an attacker to use the internal WebSockets API for CodeMeter (All versions prior to 7.00 are affected, including Version 7.0 or newer with the affected WebSockets API still enabled. This is especially relevant for systems or devices where a web browser is used to access a web server) via a specifically crafted Java Script payload, which may allow alteration or creation of license files for when combined with CVE-2020-14515.

CVE ID: **CVE-2020-16233**

CVSS v3.0 Base Score 7.5 | High | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

An attacker could send a specially crafted packet that could have CodeMeter (All versions prior to 7.10) send back packets containing data from the heap.

Remediation

Schneider Electric is establishing a remediation plan for all future versions of products impacted which do not have a fix available yet. We will update this document when the remediation is available.

Until then, customers should note that the CodeMeter installation is independent from the affected products reported in this security notification and should immediately apply the following mitigations to reduce the risk of exploit:

Schneider Electric Security Notification

Affected Products	Remediations/Mitigations
EcoStruxure Machine Expert (formerly known as SoMachine and SoMachine Motion) *All versions*	Manually update CodeMeter to version 7.10a. This version is already available for download at https://www.wibu.com/support/user Additional Mitigations • Import license files from trusted sources only. • Set up network segmentation and configure firewalls to block all unauthorized access to port 22350/TCP.
E+PLC400 *All versions*	
E+PLC100 *All versions*	
E+PLC_Setup *All versions*	
EcoStruxure Machine SCADA Expert *All Versions*	Upgrade to EcoStruxure Machine SCADA Expert versions 8.1 SP5 or 2020 which include the more secure version of CodeMeter, version 6.90a. The latest CodeMeter version 7.10a is currently being qualified. Customers should immediately implement the following additional mitigations: • Import license files from trusted sources only. • Set up network segmentation and configure firewalls to block all unauthorized access to port 22350/TCP.

To ensure you are informed of all updates to this notification 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

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. These organizations will be fully aware of this situation and can support you through the process.

https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

https://www.se.com/ww/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 **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

Schneider Electric Security Notification

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 *13 October 2020*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2020.10.11 17:02:51 -04'00'