Schneider Electric Security Notification

EcoStruxure™ Machine Expert and Modicon M218/M241/M251/M262, LMC PacDrive Eco/Pro/Pro2, HMISCU, ATV IMC Logic Controllers, SoMachine/SoMachine Motion (V2.0)

11 May 2021 (8 June 2021)

Overview

Schneider Electric is aware of multiple vulnerabilities in the 3S CODESYS third party component, which is integrated into the Schneider Electric products listed below. The affected products include Programmable Logic Controllers and the associated programming and configuration software.

Failure to apply the mitigations and remediations provided below may risk denial of service or risk potential arbitrary remote code execution.

June 2021 update: Vijeo Designer removed from the list of affected products.

Affected Products and Versions

Product	Version
EcoStruxure Machine Expert	all versions prior to V2.0
Modicon M218	all versions prior to V5.1.0.6
Modicon M241	all versions prior to V5.1.9.14
Modicon M251	all versions prior to V5.1.9.14
Modicon M262	all versions prior to V5.1.5.30
LMC PacDrive Eco/Pro/Pro2	all versions prior to V1.64.18.26
HMISCU	all versions prior to V6.2 SP11
ATV IMC	all versions
SoMachine/SoMachine Motion	all versions

Schneider Electric Security Notification

Vulnerability Details

CVE ID: **CVE-2020-10245**

CVSS v3.0 Base Score 9.8 | Critical | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CODESYS V3 web server before 3.5.15.40, as used in CODESYS Control runtime systems, has a buffer overflow.

CVE ID: **CVE-2020-6081**

CVSS v3.0 Base Score 8.8 | High | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

An exploitable code execution vulnerability exists in the PLC_Task functionality of 3S-Smart Software Solutions GmbH CODESYS Runtime 3.5.14.30. A specially crafted network request can cause remote code execution. An attacker can send a malicious packet to trigger this vulnerability.

CVE ID: **CVE-2019-13538**

CVSS v3.0 Base Score 8.6 | High | CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

3S-Smart Software Solutions GmbH CODESYS V3 Library Manager, all versions prior to 3.5.16.0, allows the system to display active library content without checking its validity, which may allow the contents of manipulated libraries to be displayed or executed.

CVE ID: **CVE-2019-9008**

CVSS v3.0 Base Score 8.8 | High | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

An issue was discovered in 3S-Smart CODESYS V3 through 3.5.12.30. A user with low privileges can take full control over the runtime.

CVE ID: **CVE-2019-9009**

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

An issue was discovered in 3S-Smart CODESYS before 3.5.15.0 . Crafted network packets cause the Control Runtime to crash.

CVE ID: **CVE-2020-7052**

CVSS v3.0 Base Score 6.5 | Medium | CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

CODESYS Control V3, Gateway V3, and HMI V3 before 3.5.15.30 allow uncontrolled memory allocation which can result in a remote denial of service condition.

Remediation

A fix for this vulnerability is available for download below.

- On the engineering workstation, update to EcoStruxure Machine Expert v2.0 or above: https://www.se.com/ww/en/product-range-download/2226-ecostruxure-machine-expert-%28somachine%29/?selected-node-id=14435955187#/software-firmware-tab
- On Modicon M218/M241/M251/M262, LMC PacDrive Eco/Pro/Pro2, HMISCU Logic Controllers, update to latest firmware version available within EcoStruxure Machine Expert v2.0. A reboot is needed.

Note: As previously announced, ATV IMC controller will be discontinued on 31st December 2021. Customers should consider upgrading to the latest product offering Modicon M262 Logic Controller to resolve this issue.

Customers should use appropriate patching methodologies when applying these patches to their systems. We strongly recommend the use of back-ups and evaluating the impact of these patches in a Test and Development environment or on an offline infrastructure. Contact Schneider Electric's Customer Care Center if you need assistance removing a patch.

If customers choose not to apply the remediation provided above, they should immediately apply the following mitigations to reduce the risk of exploit:

Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside

- Use firewalls to protect and separate the control system network from other networks
- Use VPN (Virtual Private Networks) tunnels if remote access is required
- Activate and apply user management and password features
- Limit the access to both development and control system by physical means, operating system features, etc.
- Protect both development and control system by using up to date virus detection solutions

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.

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.

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.

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 1.0 *11 May 2021*	Original Release
Version 1.0 *8 June 2021*	Vijeo Designer removed from the list of affected products. (page 1)

Product Security Office

Digitally signed by Product Security Office
Date: 2021.06.06 20:05:01 -04'00'