Schneider Electric Security Notification

CODESYS V2 Vulnerabilities in Programmable Automation Controller (PacDrive) M

10 August 2021

Overview

Schneider Electric is aware of multiple vulnerabilities disclosed by Codesys on CODESYS V2 runtime for industrial control systems, which is used in its Programmable Automation Controller (PacDrive) M products.

The Programmable Automation Controller (PacDrive) M products are legacy logic motion technology for packaging and production machines.

Failure to apply the mitigations provided below may risk buffer overflow attacks, which could result in potential denial of service condition or arbitrary remote code execution.

Affected Product and Versions

Programmable Automation Controller (PacDrive) M, all versions

Vulnerability Details

CVE ID: **CVE-2021-30186**

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

A crafted request may cause a heap-based buffer overflow in the affected CODESYS products, resulting in a denial-of-service condition.

CVE ID: **CVE-2021-30188**

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

A crafted request may cause a stack-based buffer overflow in the affected CODESYS products, resulting in a denial-of-service condition or being utilized for remote code execution.

CVE ID: **CVE-2021-30195**

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

A crafted request may cause a buffer over-read in the affected CODESYS products, resulting in a denial-of service condition.

Mitigations

The Programmable Automation Controller (PacDrive) M product has been replaced with the newer PacDrive 3 product. Customers should consider migrating to the PacDrive 3 and following the steps below to resolve these issues:

1. Migrate to PacDrive 3 controllers: https://www.se.com/ww/en/product-range/7590-pacdrive-3/?subNodeId=12367561635en_WW. Please contact your local Schneider Electric technical support for more information.

2. Download and install latest EcoStruxure Machine Expert software available here: https://www.se.com/ww/en/product-range/2226-ecostruxure-machine-expert-%28somachine%29/ to program PacDrive 3 controllers.

3. Upgrade to the latest firmware versions of PacDrive 3 controllers through Schneider Electric Software Update (SESU) Note: a reboot of the controller will be required.

If customers choose not to migrate to the most recent controllers, they should immediately apply the following mitigation to reduce the risk of exploit:

- Restrict network access to the controller via network segmentation and network access controls

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.

Schneider Electric Security Notification

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.

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 *10 August 2021*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2021.08.07 21:13:44 -04'00'