Schneider Electric Security Notification

EcoStruxure™ Panel Server Box (PAS900)

11 October 2022

Overview

Schneider Electric is aware of a vulnerability in its EcoStruxure™ Panel Server Box (PAS900) product.

The EcoStruxure™ Panel Server Box (PAS900) product is a cloud connected gateway with 4G/WIFI/Ethernet that supports Modbus TCP/RTU for south communication.

Failure to apply the remediations provided below may risk a Hole Descriptor overwrite attack or buffer overflow, which could result in arbitrary write or Denial of Service.

Affected Products and Versions

Product	Version
EcoStruxure™ Panel Server Box (PAS900)	V3.1.16 and prior

Vulnerability Details

CVE ID: **CVE-2022-30790**

CVSS v3.1 Base Score 7.3 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:H

A *CWE-787: Out-of-Bounds Write* vulnerability exists that could cause arbitrary writes when crafted malformed packets are received from a local network while U-boot is running.
Note: The CVSS score provided above is calculated in the context of EcoStruxure™ Panel Server Box.

CVE ID: **CVE-2022-30552**

CVSS v3.1 Base Score 6.2 | Medium | CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A *CWE-120: Buffer Copy without Checking Size of Input* vulnerability exists that could cause Denial of Service when a specially crafted fragmented IP Datagram with an invalid total length is received from a local network while U-boot is running.
Note: The CVSS score provided above is calculated in the context of EcoStruxure™ Panel Server Box.

Remediation

Affected Product & Version	Remediation
EcoStruxure™ Panel Server Box (PAS900) *V3.1.16 and prior*	Version 3.1.18 of Schneider EcoStruxure™ Panel Server Box (PAS900) includes a fix for these vulnerabilities and is available for download in the EMOP cloud platform: • Login to the Schneider QianLiYan (千里眼) and navigate to the EMOP device management portal. • Follow online firmware update tips and guidelines. OR • Download the latest version from EMOP cloud and do the firmware update via local web page. • Use the QuianLiYan(千里眼) to verify that the firmware was updated successfully.

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.

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 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.

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

LEGAL DISCLAIMER

THIS NOTIFICATION DOCUMENT, THE INFORMATION CONTAINED HEREIN, AND ANY MATERIALS LINKED FROM IT (COLLECTIVELY, THIS "NOTIFICATION") ARE INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND SUGGESTED MITIGATION ACTIONS, REMEDIATION, FIX, AND/OR GENERAL SECURITY RECOMMENDATIONS AND IS PROVIDED ON AN "AS-IS" BASIS WITHOUT WARRANTY OR GUARANTEE OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES RELATING TO THIS NOTIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCHNEIDER ELECTRIC MAKES NO WARRANTY THAT THE NOTIFICATION WILL RESOLVE THE IDENTIFIED SITUATION. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES OR LOSSES WHATSOEVER IN CONNECTION WITH THIS NOTIFICATION, INCLUDING DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF SCHNEIDER ELECTRIC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR USE OF THIS NOTIFICATION IS AT YOUR OWN RISK, AND YOU ARE SOLELY LIABLE FOR ANY DAMAGES TO YOUR SYSTEMS OR ASSETS OR OTHER LOSSES THAT MAY RESULT FROM YOUR USE OF THIS NOTIFICATION. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION

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.

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 *11 October 2022*	Original Release