Schneider Electric Security Notification

Easergy P5

12 July 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in its Easergy P5 product line.

The Easergy P5 is a medium voltage protection relay.

Failure to apply the mitigations or remediations provided below may risk disclosure of the device's credentials, denial of service, device reboot, or an attacker could gain full control of the relay. This could result in loss of protection of your electrical network.

Affected Product and Versions

Product	Version
Easergy P5	Firmware V01.401.102 and prior

Vulnerability Details

CVE ID: **CVE-2022-34756**

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-120: Buffer Copy without Checking Size of Input* vulnerability exists that could result in remote code execution or the crash of HTTPs stack which is used for the device Web HMI.

CVE ID: **CVE-2022-34757**

CVSS v3.1 Base Score 6.7 | Medium | CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:L/I:H/A:H

A *CWE-327: Use of a Broken or Risky Cryptographic Algorithm* vulnerability exists where weak cipher suites can be used for the SSH connection between Easergy Pro software and the device, which may allow an attacker to observe protected communication details.

CVE ID: **CVE-2022-34758**

CVSS v3.1 Base Score 5.1 | Medium | CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:L

A *CWE-20: Improper Input Validation* vulnerability exists that could cause the device watchdog function to be disabled if the attacker had access to privileged user credentials.

Schneider Electric Security Notification

Remediation

Affected Product & Versions	Remediation
Easergy P5 *Firmware V01.401.102 and prior*	V01.402.101 of the Easergy P5 Firmware includes a fix for these vulnerabilities and is available on request from Schneider Electric's Customer Care Center.

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:

CVE	Mitigation
CVE-2022-34756	Disable the device Web HMI by using the Easergy Pro to turn off the HTTPS server in the communication menu.
CVE-2022-34757	If the device firmware version is prior to V01.401.101, limit the use of Easergy Pro software to the front USB port. The option to disable SSH on the rear Ethernet board is not yet available in this version of the firmware.
	If the device firmware is V01.401.101 to V01.402.001: • Disable the SSH on the rear Ethernet port and use only Easergy Pro on the front USB port. • If you are using Easergy Pro software on the rear Ethernet port, disable SSH on the rear Ethernet port when it is not in use
CVE-2022-34758	Follow the General Security Recommendations below.

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.

Acknowledgements

Schneider Electric recognizes the following researchers for identifying and helping to coordinate a response to these vulnerabilities:

VMT	Researchers
CVE-2022-34756	U.S. Department of Energy CyTRICS researcher McKade Umbenhower –INL
CVE-2022-34758	Timothée Chauvin, Paul Noalhyt, Yuanzhe Wu at Red Balloon Security

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

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 *12 July 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.07.11 11:30:48 -04'00'