

Schneider Electric Security Notification

Easergy P5

11 January 2022 (02 March 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 credentials, denial of service, device reboot, or at attacker gaining full control of the relay. This could result in loss of protection to your electrical network.

Affected Product and Versions

Product	Version
Easergy P5	All firmware versions prior to V01.401.101

Vulnerability Details

CVE ID: **CVE-2022-22722**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

A *CWE-798: Use of Hard-coded Credentials* vulnerability exists that could result in information disclosure. If an attacker were to obtain the SSH cryptographic key for the device and take active control of the local operational network connected to the product they could potentially observe and manipulate traffic associated with product configuration.

CVE ID: **CVE-2022-22723**

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 lead to a buffer overflow causing program crashes and arbitrary code execution when specially crafted packets are sent to the device over the network. Protection functions and tripping function via GOOSE can be impacted.

Remediation

Versions 01.401.101 and 01.303.202 of the Easergy P5 Firmware include a fix for these vulnerabilities. The version to be used depends on the existing firmware in the Easergy P5. The firmware packages are available on request from Schneider Electric's [Customer Care Center](#) which will provide the guidelines on the version to be used.

For **CVE-2022-22723** only, if customers choose not to apply the remediation provided above, they should immediately apply the following mitigation to reduce the risk of exploit:

Schneider Electric Security Notification

Disable the GOOSE service of the product to reduce the risk of exposure. If GOOSE is needed for the application use it only in a secure local area network.

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 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 this vulnerability:

CVE	Researcher
CVE-2022-22723	Timothée Chauvin, Paul Noalhyt, Yuanshe 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

Schneider Electric Security Notification

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

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 11 January 2022	Original Release
Version 1.1 02 March 2022	Updated remediation instructions for clarity.