

Schneider Electric Security Notification

Easergy P40

08 February 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in its Easergy P40 product line.

The [Easergy P40](#) is a protection relay series for MV, HV and EHV protection.

Failure to apply the mitigation provided below may risk disclosure of device credentials, loss of communications, or an 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 P40 Series model numbers with Ethernet option bit as Q, R, S: P_4_ _ _ Q_ _ _ _ _ _ _ _ P_4_ _ _ R_ _ _ _ _ _ _ _ P_4_ _ _ S_ _ _ _ _ _ _ _	All PX4X firmware versions

Vulnerability Details

CVE ID: **CVE-2022-22813**

CVSS v3.1 Base Score 7.1 | High | CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

A *CWE-798: Use of Hard-coded Credentials* vulnerability exists. If an attacker were to obtain the TLS cryptographic key and take active control of the Courier tunneling communication network, they could potentially observe and manipulate traffic associated with product configuration.

OpenSSL Vulnerabilities

CVSS v3.1 Base Score 7.1 | High | CVSS:3.1/AV:A/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

An older version of Open SSL, a cryptographic cipher suite, is integrated in the Easergy P40 product. If an attacker were to take active control of the Courier tunneling communication network and exploit vulnerabilities in this library it may risk disclosure of device credentials, denial of service, or an attacker gaining full control of the relay. The CVSS score provided above reflects the worst case exploit of the known vulnerabilities present in the library.

Schneider Electric Security Notification

Mitigation

These vulnerabilities impact the secure Courier tunneling communication over Ethernet. This communication is only used for commissioning between the IED and Easergy Studio software. It is recommended to only use Courier tunneling with Easergy Studio software in a secured network and disable the logical port by disabling “Courier Tunnel” in settings when not in use.

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>

Schneider Electric Security Notification

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 <i>08 February 2022</i>	Original Release
---	-------------------------