Cybersecurity Vulnerability Disclosure

Overview

Schneider Electric has become aware of multiple vulnerabilities in the Ezylog product marketed in Italy for use in monitoring solar power inverters.

Vulnerability Overview

The vulnerability types identified include hard-coded credentials, SQL injection, command execution, and broken session enforcement.

Product(s) Affected

The product(s) or product lines affected include:

- Schneider Electric Ezylog, P/N PVSNVLOG, all versions (note that this product was only sold and supported in Italy)

Vulnerability Details

- Ezylog installs with a default password. This allows attackers to access the program or system and gain privileged access.
- Ezylog contains a flaw that may allow an attacker to carry out an SQL injection attack. This may allow an attacker to inject or manipulate SQL queries in the back-end database, allowing for the manipulation or disclosure of arbitrary data.
- Attackers can exploit Ezylog's "ping.php" page to execute arbitrary commands on the device, with administrative privileges. Thus it is possible to leverage traditional command-injection techniques to inject arbitrary commands.
- Ezylog's software does not verify whether a user who accesses the management web pages is associated with a properly authenticated session. This permits vulnerabilities to be exploited by unauthenticated attackers.

Mitigation

A patch is available that eliminates the identified vulnerabilities. Product owners should install this patch on their installed units. To access the patch, users should use the Update Firmware option in their product. They can navigate to the Update Firmware by selecting System Configuration, then System Setup, then System.

Ezylog is a monitoring and reporting device. It is designed to collect information from solar inverters, store the collected data, and present it via graphs, trends, and reports. Additionally, any alarm conditions programmed will send alerts to identified users. This product is not designed to control or force any action on the solar inverters it connects to or take any actions beyond email alerts or storing of data. As with all internet-facing devices, Schneider Electric strongly recommends the user protect access to the device through a properly configured firewall.

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact Schneider Electric's Corporate Product CERT at cybersecurity@schneider-electric.com (include the word "cybersecurity" in the Subject line)

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com