Overview

Schneider Electric is aware of a vulnerability in the Power SCADA Operation product.

Affected Product(s)

Power SCADA Operation 9.0 (including all associated Cumulative Updates)
Power SCADA Expert 8.2 (including all associated Cumulative Updates)
Power SCADA Expert 8.1 (including all associated Cumulative Updates)
Power SCADA Expert 8.0 (including all associated Cumulative Updates)
Power SCADA Expert 7.4 (including all associated Cumulative Updates)
Power SCADA Expert 7.3 (including all associated Cumulative Updates)

Vulnerability Details

CVE: **CVE-2019-13537**
CVSS v3.0 Base Score 7.5 | (High) | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

A CWE-121 Stack-based Buffer Overflow vulnerability exists which could cause a server side crash when an attacker induces a buffer overflow.

The IEC870IP driver for Power SCADA Operation and other mentioned versions above has a buffer overflow that could cause a server-side crash. This driver handles communication for connected products using the IEC 60870-5-104 protocol.

Remediation

This vulnerability is fixed in version v4.15.00 and is available for download below:

[https://schneider-electric.app.box.com/s/4r7woqy9pyhw3z8sbbh1m9se9l4ojv2x](https://schneider-electric.app.box.com/s/4r7woqy9pyhw3z8sbbh1m9se9l4ojv2x)

Customers using the IEC870IP driver v4.14.02 and earlier are affected and should upgrade to the IEC870IP driver v4.15.00 as soon as possible. This vulnerability impacts only the IEC870IP driver and not the core Power SCADA Operation software. As a result, an upgrade of the Power SCADA Operation version is not necessary.
The IEC870IP protocol does not provide for authentication and its use should be evaluated. For information regarding how to secure Industrial Control Systems please reference NIST SP800-82r2.

Product Information

Power SCADA Operation is engineered to help facilities like data centers, hospitals, industrials, airports and electro-intensive operations maximize uptime. With rich data integration from connected devices, PSO's unique capabilities provide real-time situational awareness, and offer a high performance, cyber-resilient solution for your specialized power networks.

Product Category - Low Voltage Products and Systems
Learn more about Schneider Electric’s product categories here: www.schneider-electric.us/en/all-products

How to determine if you are affected
If you are using the above mentioned versions of Power SCADA Expert or Power SCADA Operation.

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place so that no unauthorized person would have access to the ICS and safety controllers, peripheral equipment or the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. should be scanned before use in the terminals or any node connected to these networks.
- Laptops that have connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or 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), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.
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, please contact your local Schneider Electric representative and/or Schneider Electric Industrial Cybersecurity Services. These organizations will be fully aware of this situation and can support you through the process.

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page


Legal Disclaimer

THIS DOCUMENT IS 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 OF ANY KIND. SCHNEIDER ELECTRIC DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL SCHNEIDER ELECTRIC BE LIABLE FOR ANY DAMAGES WHATSOEVER 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. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. 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 make the most of their energy and resources, 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 about our Meaningful Purpose, Inclusive and Empowered values.

www.se.com