Schneider Electric Security Notification

Security Notification – PowerSCADA Expert

11 June 2019

Overview

Schneider Electric is aware of a vulnerability in the PowerSCADA Expert product.

Affected Product(s)

The following versions are affected:

- PowerSCADA Expert 7.30
- PowerSCADA Expert 7.40
- PowerSCADA Expert 8.0 without Service Release 1

Note: Customers using PowerLogic SCADA 7.20 and earlier versions, as well as PowerSCADA Expert 8.0 with Service Release 1, PowerSCADA Expert 8.1, PowerSCADA Expert 8.2 and Power SCADA Operation 9.0 versions, are not affected but should upgrade to Power SCADA Operation 9.0 to receive the latest product improvements.

Vulnerability Details

CVE: **CVE-2019-10981**

CVSS v3.0 Base Score 6.5 | (Medium) | CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

In CitectSCADA 7.30 and 7.40, a vulnerability has been identified that may allow an authenticated local user access to Citect user credentials. This also affects PowerSCADA Expert 7.30, PowerSCADA Expert 7.40 and PowerSCADA Expert 8.0 without Service Release 1.

Remediation

At the time of this publication the latest release of Power SCADA Operation is 9.0 (formerly PowerSCADA Expert and PowerLogic SCADA). Customers are strongly encouraged to upgrade to the latest release using the download link below:

https://schneider-electric.box.com/shared/static/8hucqox5bshzbjf9uun3a6orzc3e5r2u.iso

Schneider Electric Security Notification

SHA256 checksum:
FB2F5DC91AFB2E1E4CA394DD23CF3342C202AD39E204900CCE95DF055E328D4A

Product Information

Power SCADA Operation enables Facilities teams in Power Critical Facilities to monitor, control, and troubleshoot issues in real-time with their electrical distribution systems to maximize power reliability and operational efficiency.

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

All customers using version PowerSCADA Expert 7.30, PowerSCADA Expert 7.40 and PowerSCADA Expert 8.0 without Service Release 1 are affected.

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.

Schneider Electric Security Notification

For More Information

This document is intended to help provide an overview of the identified situation and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

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

If you require additional support, Schneider Electric Industrial Cybersecurity Services team are available to help. Please visit: https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND MITIGATION ACTIONS, AND IS PROVIDED ON AN "AS-IS" BASIS AND IS NOT INTENDED AS A WARRANTY OR GUARANTEE OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. 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.

Revision Control:

Version 1	Original Release
11 Jun 2019	