# Important Security Notification

## Security Notification – PowerSCADA Anywhere

22-June-2017

## Overview

Schneider Electric® has become aware of multiple vulnerabilities in the PowerSCADA Anywhere software.

## Vulnerability Overview

The vulnerabilities identified include:

- Cross-Site Request Forgery (CSRF) on the Secure Gateway component of PowerSCADA Anywhere for multiple state-changing requests. This type of attack requires some level of social engineering in order to get a legitimate user to click on or access a malicious link/site containing the CSRF attack.
- Ability to specify Arbitrary Server Target Nodes in connection requests to the PowerSCADA Anywhere Secure Gateway and PowerSCADA Anywhere Server components.
- Use of outdated cipher suites and improper verification of peer SSL Certificate
- Ability to escape out of remote PowerSCADA Anywhere applications and launch other processes.

The vulnerabilities, if exploited, could allow a malicious entity to:

- Perform actions on behalf of a legitimate user
- Perform network reconnaissance
- Gain access to resources beyond those intended with normal operation of the product

Schneider Electric takes these vulnerabilities very seriously and we have devoted resources to immediately investigate and address these issues. We believe it is critical to consider the whole picture, including safety, security and reliability. Any patches/solutions/mitigations we release will be carefully tested to ensure that they can be deployed in a manner that is both safe and secure.

## Product(s) Affected

The product(s) affected:

- Version 1.0 of PowerSCADA Anywhere redistributed with PowerSCADA Expert v8.1 and PowerSCADA Expert v8.2

## Vulnerability Details

The vulnerabilities, if exploited, could allow a malicious entity to:

- Perform actions on behalf of a legitimate user
- Perform network reconnaissance
- Gain access to resources beyond those intended with normal operation of the product

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference, they should be adapted by individual users as required.

- Cross Site Request Forgery
    - Overall CVSS Score: 8.1 (High)
    - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N
    - CVE-2017-7969: http://www.cve.mitre.org/cgibin/cvename.cgi?name=2017-7969
- Arbitrary Server Target Nodes
    - Overall CVSS Score: 6.5 (Medium)
    - CVSS:3.0/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
    - CVE-2017-7970: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7970
- Outdated Cipher Suites/Cert Verification
    - Overall CVSS Score: 5.3 (Medium)
    - CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N
    - CVE-2017-7971: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7971
- Escaping PowerSCADA Application
    - Overall CVSS Score: 5.5 (Medium)
    - CVSS:3.0/AV:A/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
    - CVE-2017-7972: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-7972

## Mitigation

Existing customers: Schneider Electric strongly recommends that existing customers upgrade their systems as soon as possible. The following provides links to instructions for addressing software that is at potential risk to this vulnerability:

- PowerSCADA Anywhere Version 1 used with PowerSCADA Expert v8.2 and PowerSCADA Expert v8.1: Uninstall PowerSCADA Anywhere (from Add/Remove Programs). Then install PowerSCADA Anywhere Version 1.1 available in the following location: https://schneider-electric.box.com/shared/static/3tvcc115kax8volhd8i13e4wg5k1sdel.iso *(SHA256 checksum to verify download of .iso file): D0FB69453EC85B7586801CA0A7BCCD86B4A4CFB3DFC82B4271AE654A1978EAE0*

In addition to installing the provided security patch, further steps can be taken to harden the system:

- Configure the PowerSCADA Anywhere Secure Gateway's HTTP Origin Header whitelist to match your environment's URL(s) used for accessing the Secure Gateway. This address may be one or more of the IP, Machine Name, or Fully Qualified Domain Name where the Secure Gateway is hosted. The address may also be that of a Load Balancer or Proxy, if the Secure Gateway is deployed that way.
- Configure the PowerSCADA Anywhere Secure Gateway's whitelists to restrict access to expected clients IPs, as well as to restrict access from the Secure Gateway to only expected internal server hosts. For an additional defense-in-depth layer, you can further use the Windows OS-level Firewall (or zone firewalls) to restrict communication among only the expected nodes.
- If using self-signed certificates, configure the PowerSCADA Anywhere Secure Gateway machine to trust the PowerSCADA Anywhere Server certificate.
- Depending on your organization's requirements, you can further configure the PowerSCADA Anywhere Secure Gateway to restrict the usable TLS Protocols. For an additional defense-in-depth layer, TLS protocols and cipher suites can also be restricted at the Operating System level through the use of 3rd party tools such as IISCrypto.
- Ensure that you create unique user accounts with minimal privileges dedicated to accessing PowerSCADA applications remotely. OS Group Policy Objects (GPO) can be used to further restrict what those unique user accounts are allowed to do. For an example configuration that disables task manager from being launched in a Remote App connection, follow the steps here: https://social.technet.microsoft.com/Forums/office/en-US/35dd3cd6-cc67-476f-82e2-058293e6f657/how-do-i-disable-task-manager-for-users-only?forum=winserverTS

## 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 your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

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**

Product Security Office

Digitally signed by Product Security Office
DN: cn=Product Security Office, o=Schneider Electric, ou=Global Technology, email=cybersecurity@schneider-electric.com, c=US
Date: 2017.06.21 16:22:22 -04'00'