Security Notification – PowerSCADA Expert Licensing Brick

24-March-2017

Overview

Schneider Electric® has become aware of a vulnerability in the Flexera FlexNet Publisher component used in the Schneider Electric Floating License Manager software that is used with PowerSCADA Expert.

Vulnerability Overview

Flexera Software reported a vulnerability to its Flexera FlexNet Publisher, CVE-2016-6273. This 3rd Party Component is used within the Schneider Electric Floating License Manager. This vulnerability could permit a remote attacker to cause a denial of service.

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:

- PowerSCADA Expert 8.1
- PowerSCADA Expert 8.0 SR1
- PowerSCADA Expert 7.40
- PowerSCADA Expert 7.30
- PowerSCADA Anywhere

Vulnerability Details

This vulnerability could permit a remote attacker to cause a denial of service.

Overall CVSS v3 Base Score: 7.5 (High)
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Mitigation

To exploit this issue, an attacker would need network access to the server hosting PowerSCADA Expert or PowerSCADA Anywhere.

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 Expert 8.1: Apply the latest PowerSCADA 8.1 hotfix update, available in the following location:
  https://schneider-electric.box.com/shared/static/z9qienrkijflb677sxxxb9am2ixne5qd.zip
- PowerSCADA Anywhere: Uninstall Floating License Manager (from Add/Remove Programs). Then install Floating License Manager v1.9.10.0 available in the following location:
  https://schneider-electric.box.com/shared/static/m755rgbkc2rkqjnnwwo0zxdfu9czvz75.zip
- PowerSCADA Expert 8.0 SR1: Apply the latest PowerSCADA 8.0 SR1 hotfix update, available in the following location:
  https://schneider-electric.box.com/shared/static/n3cidl8r4s2xmvpgk9lqcudtewft5bi0.zip
- PowerSCADA Expert 8.0, 7.40, 7.30: The Flexera Software FlexNet components were not used in these versions of PowerSCADA Expert. However, as a precaution, we recommend that users uninstall Floating License Manager and License Manager (from Add/Remove Programs), if they have been installed.

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

Schneider Electric is the global specialist in energy management and automation. With revenues of ~€25 billion in FY2016, our 160,000+ employees serve customers in over 100 countries, helping them to manage their energy and process in ways that are safe, reliable, efficient and sustainable. From the simplest of switches to complex operational systems, our technology, software and services improve the way our customers manage and automate their operations. Our connected technologies reshape industries, transform cities and enrich lives. At Schneider Electric, we call this **Life Is On**.

www.schneider-electric.com