Security Notification (Version 1.1) – EcoStruxure Power Monitoring Expert, EcoStruxure Building Operation & StruxureWare PowerSCADA Expert

07-Nov-2017

Overview

Schneider Electric has become aware of a vulnerability in a third-party software control in EcoStruxure Power Monitoring Expert and EcoStruxure Building Operation - Energy Expert (formerly known as Power Manager).

Vulnerability Overview

The vulnerability is a cryptographic weakness in Telerik.Web.UI.dll. that can be exploited and could lead to the disclosure of encryption keys (Telerik.Web.UI.DialogParametersEncryptionKey and/or the MachineKey).

Product(s) Affected

The product(s) affected:

- EcoStruxure Power Monitoring Expert 7.2.x, 8.0, 8.1, 8.2
- EcoStruxure Building Operation - Energy Expert (formerly known as Power Manager)1.x

- StruxureWare PowerSCADA Expert versions 8.0, 8.1, 8.2, when using Advanced Reporting & Dashboards Module ONLY

Vulnerability Details

The vulnerability is a cryptographic weakness in Telerik.Web.UI.dll. that can be exploited and could lead to the disclosure of encryption keys (Telerik.Web.UI.DialogParametersEncryptionKey and/or the MachineKey).

Knowledge of these keys in web applications using Telerik UI for ASP.NET AJAX components can lead to:

- cross-site-scripting (XSS) attacks
- leak of MachineKey
- compromise of the ASP.NET ViewState
- arbitrary file uploads/downloads

Overall CVSS Score: 9.8 (Critical)

(CVSS V3 Vector): CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (legend)

CVE ID: CVE-2017-11357 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11357

Mitigation

The quickest most effective way to mitigate against this vulnerability is to edit a file called web.config, located in the [PME Install Directory]\web directory. The edit required depends on which pipeline mode is being used. To determine pipeline mode:

1. Go to IIS Manager select Application Pools and click on the WebReporterApp Pool and look at the pipeline mode for WebReporter App Pool.
2. Click on 'Basic Settings' and look at 'Managed pipeline mode'
3. Once pipeline mode has been determined, open Web.config from [PME Install Directory]\web

If the pipeline is in 'integrated' mode, paste the snippet below under the <handlers> node in <system.webServer>:

```
<remove name="Telerik_Web_UI_WebResource_axd" />

<add name="Telerik_Web_UI_WebResource_axd" path="Telerik.Web.UI.WebResource.axd"
type="Telerik.Web.UI.WebResource" verb="GET" preCondition="integratedMode" />
```

If the pipeline is in 'classic' mode, paste the snippet below under the <httpHandlers> node in <system.web>:

```
<add path="Telerik.Web.UI.WebResource.axd" type="Telerik.Web.UI.WebResource"
verb="GET" validate="false" />
```

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

Revision Control:

Version 1.0 *07 November 2017*	Original Release
Version 1.1 *07 November 2017*	StruxureWare PowerSCADA Expert added as an impacted product

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: 2017.11.07 17:05:37 -05'00'