



Important Security Notification

Floating License Manager Security Update

~~3145~~-Jan-2014

Overview

Schneider Electric has become aware of an “unquoted service path” vulnerability in the Schneider Electric Floating License Manager.

Vulnerability Overview

The unquoted service path vulnerability affects one of the services installed by the Floating License Manager. This vulnerability could allow attackers to start malicious programs as Windows services.

Product(s) Affected

The product(s) or product lines affected include:

- Schneider Electric Floating License Manager, Versions V1.0.0 through V1.4.0. [This license manager is used in Power Monitoring Expert, Struxureware process Expert \(PES\), Struxureware process Expert libraries, Vijeo Citect \(SCADA\) and Vijeo Citect Historian](#)

Vulnerability Details

- When the executable path of a service contains blanks, attackers can exploit this to start malicious programs as Windows services. To avoid this, such service paths in the registry must be surrounded with quotes.

Mitigation

When one of the above mentioned versions of Floating License Manager is installed on your system, Schneider Electric Software Update will inform you on an update for this program:

Important Security Notification

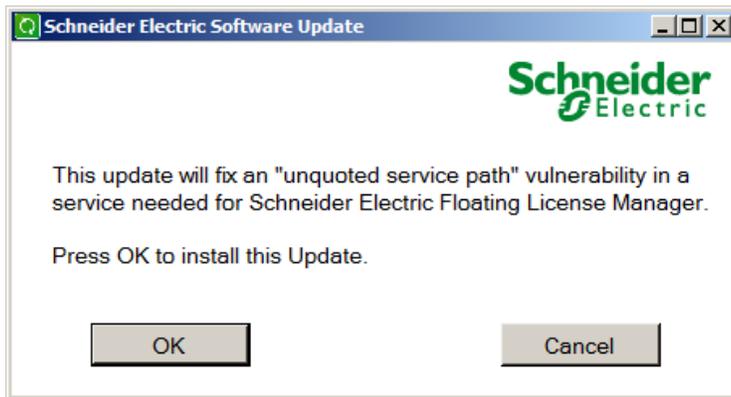
New updates & messages

▼ Schneider Electric Floating License Manager V1.4.0.0

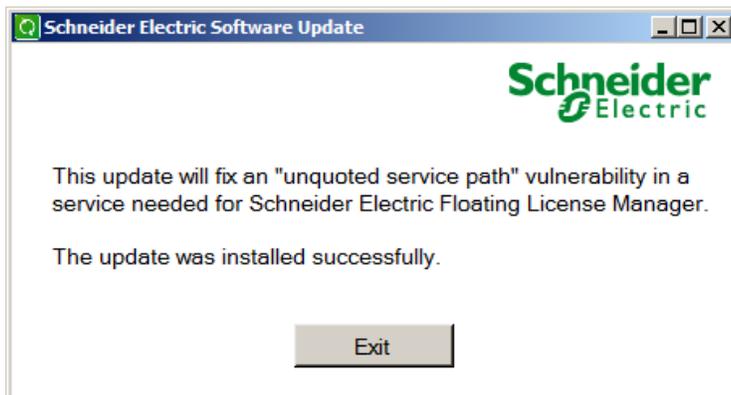
Important Updates	Date	Size
<input type="checkbox"/> ▼ SWLic_2014_01 (Security Update for Schneider Electric Floating License Manager) *	2014-01-08	26 KB

This update is fixing an "unquoted service path" vulnerability in one of the services used by Schneider Electric Floating License Manager.

When you download and install this update, you will see the following dialog (it is only provided in English):



After pressing OK, the needed change in your registry is done and you get informed that the update was installed successfully:





Important Security Notification

Press on Exit to finish the installation of this security update.

Note that this update does not install new dlls, it only modifies one entry in the registry. Because this entry is protected, this update has to be **executed with administrator rights**.

It is important to confirm that your computer is running the Schneider Electric Software Update utility and has access to the internet to retrieve it's required updates.

Alternatively, you can download the patch from the following location:

https://www.update.schneider-electric.com/download/SystemConsistency/SWLic/2014_01_Security_FLM/FixUnquotedServicePathForFLM.exe

Release notes are published at the following location:

https://www.update.schneider-electric.com/download/SystemConsistency/SWLic/2014_01_Security_FLM/ReleaseNotes_Update_SWLic_2014_01.pdf

Field Code Changed

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

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential. www.schneider-electric.com