Important Security Notification

Vulnerability Disclosure - OPC Factory Server Buffer Overflow

March 25, 2014

Overview

Schneider Electric has become aware of vulnerability in the OPC Factory Server (OFS) product line.

Vulnerability Overview

Incorrect parsing in the OPC Automation 2.0 Server Object (ActiveX) can result in a buffer overflow error. This has been shown to occur when the control is used in Internet Explorer 6.

Product(s) Affected

The products affected include:

- TLXCDSUOFS33 - V3.5 and previous
- TLXCDSTOFS33 – V3.5 and previous
- TLXCDLUOFS33 – V3.5 and previous
- TLXCDLTOFS33 – V3.5 and previous
- TLXCDLFOFS33 – V3.5 and previous

Vulnerability Details

The vulnerability is related to the parsing of arguments in the Connect() and GetOPCServers() functions when called with long arguments.

Mitigation

Schneider Electric has developed a fix to resolve this issue. In order to patch the installation in the field, install OFS V3.5 SP1 patch available on Schneider Electric web site at the following URL

http://www.schneider-electric.com/download/WW/EN/results/0/0/8336568-OPC-Factory-Server/0/?showAsIframe=true

This version includes a rebuilt opcautosa2.dll that includes a patched version of the OLE2T macro from Microsoft to resolve the issue.

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