# OPC Factory Server (OFS) Test Client Security Update

31-Jan-2014

## Overview

Schneider Electric has become aware of a vulnerability in the C++ sample client supplied with the OFS product line.

## Vulnerability Overview

The parsing of the configuration file by the C++ sample client exposes a buffer overflow vulnerability that may lead to remote code execution.

## Product(s) Affected

The product(s) or product lines affected include:

- TLXCDSUOFS33 - V3.35
- TLXCDSTOFS33 – V3.35
- TLXCDLUOFS33 – V3.35
- TLXCDLTOFS33 – V3.35
- TLXCDLFOFS33 – V3.35

## Vulnerability Details

- When a malformed configuration file is parsed by the C++ sample client it may cause a buffer overflow, using a specially crafted configuration file it is possible to execute code on the PC.
- This vulnerability could allow an attacker that was able to modify the sample client configuration file to start malicious programs or execute code on the PC when the sample client opened the configuration file.
- The sample client is supplied for sample purposes only and is not recommended for use in a production environment. The main software supplied with the OFS is the OFS OPC Server which provides access to Schneider Electric devices.

- The following CVSS score has been provided for this vulnerability :
  6.8 (AV:L/AC:L/Au:S/C:C/I:C/A:C)

## Mitigation

Schneider Electric has resolved the issue in the sample client supplied with OFS V3.4 and above.

We recommend customers to upgrade to OFS V3.4 or later (V3.5 is currently available). The latest version of OFS can be found at www.schneider-electric.com

Customers that are not presently able to upgrade may choose to remove the C++ sample client from affected computers, provided it is not required for operations.

## 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