Important security notification

SCADA Expert ClearSCADA File Parsing Vulnerability

SEVD 2014-024-01

January 24, 2014

Schneider Electric® has become aware of a vulnerability involving the StruxureWare SCADA Expert ClearSCADA software.

The vulnerability identified:

- An input project-file validation vulnerability is present in the KepServer V4 component from Kepware present within the PLC Driver in SCADA Expert ClearSCADA versions released prior to January 2014.
- The PLC Driver is an optional component that requires selection during installation. Most ClearSCADA users have not enabled this PLC Driver, however may have installed this component during a full installation.
- There is no evidence that this vulnerability has been exploited in a production environment.

Details on Products Affected

The following supported software versions are affected by the SCADA Expert ClearSCADA File Parsing vulnerability:

- ClearSCADA 2010 R2 (build 71.4165) Released May 2011
- ClearSCADA 2010 R2.1 (build 71.4325) Released November 2011
- ClearSCADA 2010 R3 (build 72.4560) Released June 2012
- ClearSCADA 2010 R3.1 (build 72.4644) Released September 2012
- SCADA Expert ClearSCADA 2013 R1 (build 73.4729) Released December 2012
- SCADA Expert ClearSCADA 2013 R1.1 (build 73.4832) Released March 2013
- SCADA Expert ClearSCADA 2013 R1.1a (build 73.4903) Released June 2013
- SCADA Expert ClearSCADA 2013 R1.2 (build 73.4955) Released July 2013
- SCADA Expert ClearSCADA 2013 R2 (build 74.5094) Released December 2013

Details on workarounds or planned fix dates

Schneider Electric takes these vulnerabilities very seriously and to simplify customers handling of security patches for 3rd party components has completed the removal of this component in future versions of SCADA Expert ClearSCADA.

Customers using this PLC Driver were informed in September 2012 of the planned removal of this component from ClearSCADA. At that time, Schneider Electric recommended that customers should uninstall this component and migrate to an external installation of KepServerEX V5, available direct from Kepware, to facilitate future security patches.

Kepware has confirmed that this vulnerability is not present in V5 of KepServerEX.

A documented procedure and software tool has been prepared to assist with this migration and will be provided free of charge from Schneider Electric on request.

General Recommendations

Schneider Electric has been designing industrial automation products for many years; Schneider Electric follows, and recommends to its customers, industry best practices in the development and implementation of control systems. This recommendation includes a Defense in Depth approach to secure an Industrial Control System.

Download our cybersecurity whitepaper from www.schneider-electric.com. See Support > Cybersecurity

Schneider Electric advises all ClearSCADA users to take steps to secure the interfaces to the ClearSCADA system.

Support CVSS Scoring

CVSS scores are a standard way of ranking vulnerabilities and are provided for reference based on a typical control system. They should be adapted by individual users as required.

CVSS Base Score: 6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)

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