SCADA Expert ClearSCADA Self Signed Certificate Vulnerability

SEVD-2014-241-02A

October 6, 2014

Overview

Schneider Electric has become aware of a vulnerability in the SCADA Expert ClearSCADA product line.

Vulnerability Overview

The vulnerability identified is as follows:

- The default self-signed web certificate provided with ClearSCADA uses MD5; a deprecated and weak signing algorithm.

Product(s) Affected

The product(s) or product lines affected include:

- 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
- SCADA Expert ClearSCADA 2013 R2.1 (build 74.5192) Released March 2014
- SCADA Expert ClearSCADA 2014 R1 (build 75.5210) Released April 2014

Vulnerability Details

- The default self-signed security certificate provided with SCADA Expert ClearSCADA versions prior to September 2014 uses a deprecated and weak signing algorithm, allowing for decryption of SSL content and leakage of potentially sensitive system information.
- ClearSCADA customers who have obtained a valid security certificate from a certificate authority are not exposed to this vulnerability.
- CVSS Base Score 4.3; Vector (AV:N/AC:M/Au:N/C:P/I:N/A:N).

Mitigation

Schneider Electric advises all ClearSCADA users to take steps to secure the interfaces to the ClearSCADA system. Customers should always obtain a signed web certificate from a certified authority before deploying ClearSCADA Web Server in a production environment.

Update for revision A:

To assist customers who are currently using self-signed certificates, a standalone utility is available which can be used to generate and deploy a new self-signed certificate (signed using an SHA signing algorithm). This utility is recommended for existing ClearSCADA systems subject to this vulnerability, removing the need to upgrade the ClearSCADA software and perform a manual generation of a new certificate. This utility is available within the Software Downloads section of the following ClearSCADA Resource Center page:

http://resourcecenter.controlmicrosystems.com/display/CS/SCADA+Expert+ClearSCADA+Support

In addition, Schneider Electric has corrected the vulnerability in the following immediate Service Packs:

- ClearSCADA 2010 R3.2 Released Oct. 2014
- SCADA Expert ClearSCADA 2014 R1.1 Released Oct. 2014

End of Update for Revision A

Service Packs for other supported versions will be made available in due course.

If you do wish to upgrade to a new ClearSCADA Service Pack, please contact your local Schneider Electric office for latest software version for ClearSCADA; alternatively these new

versions are available for direct download from the Schneider Electric website. To update your license (not required when upgrading to a Service Pack of the same version), customers are required to complete and submit an online form available here:

http://resourcecenter.controlmicrosystems.com/display/CS/StruxureWare+SCADA+Expert+ClearSCADA+Update+Request+Form

General instructions on how to upgrade your ClearSCADA license (if required) are available here:

http://resourcecenter.controlmicrosystems.com/display/CS/Updating+Your+ClearSCADA+License

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