SCADA Expert ClearSCADA Security Vulnerabilities

SEVD-2014-241-01B

October 6, 2014

Overview

Schneider Electric has become aware of a number of security vulnerabilities in the StruxureWare SCADA Expert ClearSCADA product line.

Vulnerability Overview

The vulnerabilities identified are as follows:

1. SCADA Expert ClearSCADA versions released prior to September 2014 may be vulnerable to specific Web Cross-Site Request Forgery attacks, which could be exploited to trick a user with system administration privileges logged in via the WebX client interface to unknowingly execute a remote shutdown of the ClearSCADA Server.

2. SCADA Expert ClearSCADA installations which have not been set up with correct permissions on the database can expose potentially sensitive system information to users without requiring logon credentials.

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

1. The ClearSCADA WebX Server configuration provides an option to “Allow database shutdown via WebX”, allowing system administration users logged in via WebX to remotely initiate a shutdown of the ClearSCADA Server. This functionality, in conjunction with the vulnerability to specific Web Cross-Site Request Forgery attacks, could be exploited to trick a user with system administration privileges logged in via the WebX client interface to unknowingly execute a remote shutdown of the ClearSCADA Server. In a Lone Server system configuration without redundancy, this would cause the ClearSCADA system to become inoperable.
    - ClearSCADA customers not using the Web Server are not exposed to this vulnerability.
    - There is no evidence that this vulnerability has been exploited in a production environment.
    - CVSS Base Score 4.9; Vector (AV:N/AC:H/Au:S/C:N/I:N/A:C).

2. The Guest user account within ClearSCADA is provided read access to the ClearSCADA database for the purpose of demonstration for new users. This default security configuration is not sufficiently secure to be adopted for systems placed into a production environment, and can potentially expose sensitive system information to users without requiring logon credentials.
    - There is no evidence that this vulnerability has been exploited in a production environment.
    - CVSS Base Score 6.4; Vector (AV:N/AC:L/Au:N/C:P/I:P/A:N).

Mitigation

Schneider Electric advises all ClearSCADA users to take steps to secure the interfaces to the ClearSCADA system. The ClearSCADA database security configuration should be reviewed and updated to limit all system access to authorized users only. The access permissions of existing users should be reduced to only those required by their role (e.g. removing any higher level System Administration privileges from Operations or Engineering users), and specific accounts should be created with appropriate permissions for performing System Administration tasks.

1. Existing ClearSCADA customers using WebX can protect their system from Cross-Site Request Forgery attacks by disabling the ‘Allow database shutdown via WebX’ option within the ClearSCADA Server Configuration utility.

2. Existing ClearSCADA customers should take measures to ensure their system does not grant any system access until users have supplied a valid username and password.

Note: Schneider Electric has corrected the default user security permissions and will make these available in all subsequent releases of SCADA Expert ClearSCADA; however upgrading an existing vulnerable installation to a new version will not affect existing configured database security permissions. Therefore, the measures suggested here are strongly recommended for all users.

Updated for revision B:

Schneider Electric has corrected these vulnerabilities in the following Service Packs:

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

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

New Service Packs for ClearSCADA are available for download here:

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

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

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

End of Update for revision B

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