

Technical Support Bulletin – Security Advisory

Overview

Schneider Electric Telemetry & Remote SCADA Solutions (formerly Control Microsystems) conducts regular security vulnerability assessments of current and previous versions of its ClearSCADA enterprise software to ensure optimal performance within the highest standards of software security. Collaborating with external IT vulnerability assessment organizations, our team performs thorough assessments using the latest techniques available. During a recent security assessment, the team has identified one potential security issue that affects ClearSCADA. This issue has not been reported by customers and there have been no reported instances of this issue being used against installed ClearSCADA systems.

This bulletin outlines the identified security issue and its resolution.

Affected Products

- ClearSCADA 2010 R1.0
- ClearSCADA 2009
- ClearSCADA 2007
- ClearSCADA 2005

This Advisory applies to all versions of SCX (from Serck UK or Serck Aus) that are older than and including the following (these SCX versions contain ClearSCADA in the bundle):

- SCX Version 6.69 R1
- SCX Version 6.68
- SCX Version 6.67

Identified Issues & Potential Impact

Issue:

ClearSCADA provides a Web interface for remote connections. When an exception occurs in the dbserver.exe file during the authentication process, ClearSCADA enters the "Safe Mode" of operation. This exposes its diagnostic functions to remote users without requiring a valid login.

Impact: Successful exploitation of this vulnerability allows an attacker access to diagnostic information without proper authentication.

Resolution

Schneider Electric Telemetry & Remote SCADA Solutions (formerly Control Microsystems) has corrected this issue with the release of ClearSCADA 2009 R2.4 as well as of ClearSCADA 2010 R1.1 and later. We strongly recommend that all ClearSCADA users upgrade their licences as soon as possible.

ClearSCADA upgrades are free of charge with a valid SCADACare support agreement with Schneider Electric Telemetry & Remote SCADA Solutions (formerly Control Microsystems). Additional information about software updates can be found here:

<http://www.clearscada.com/services-support/software-updates/>

To upgrade, customers are required to complete and submit an online form available here

<http://www.controlmicrosystems.com/form/CMIform.html>

General instructions on how to upgrade your ClearSCADA license are available here

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

Detailed instructions on how to upgrade a ClearSCADA license are available here:

Upgrading to ClearSCADA 2010 R2

<http://resourcecenter.controlmicrosystems.com/display/public/CS/ClearSCADA+2010+R2+Upgrade+Strategy>

Upgrading to ClearSCADA 2009 R2

<http://resourcecenter.controlmicrosystems.com/display/public/CS/ClearSCADA+2009+R2+Upgrade+Strategy>

Contact your Regional Sales Manager or your Schneider Electric Telemetry & Remote SCADA Solutions (formerly Control Microsystems) representative for additional information. Users can also contact the factory directly at 1-888-267-2232.

Corrected Software Versions

ClearSCADA 2010 R1.1

ClearSCADA 2010 R2

ClearSCADA 2009 R2.4

These corrections also apply to SCX from version:

SCX Version 6.69 R2

Security Recommendations

Schneider Electric Telemetry & Remote SCADA Solutions (formerly Control Microsystems) is advising all ClearSCADA users to take steps to secure the interfaces to the ClearSCADA system. The following guidelines should be taken as a starting point only in establishing an appropriate level of system security:

- Limit access to the server and server network to only trusted networks and users.
- Disable logons on ClearSCADA non-secure ports. This setting can be found under System Configuration ->WebX in the server configuration window.
- Install a WebX security certificate from a trusted authority.
- Upgrade the ClearSCADA server to ClearSCADA 2010 R1.1 or newer. ClearSCADA 2009 and earlier will not be patched.

Next Steps

We strongly recommend that all ClearSCADA users upgrade their licences as soon as possible. The Department of Homeland Security National Cyber Security Division's Control Systems Security Program (CSSP) is aware of the issues reported above. An advisory from the CSSP's Industrial Control Systems Cyber Emergency Response Team regarding ClearSCADA will be publicly released within three months from this note. For more information, please go to http://www.us-cert.gov/control_systems/ics-cert/

Further Information

For upgrade requests, please complete and submit the online form available here: <http://www.controlmicrosystems.com/form/CMIform.html> or email scadacare@controlmicrosystems.com

For technical support questions, please contact:

Region	Hours	Phone No.	Email
Americas	Mon-Fri 8am - 6:30pm EST	1-888-226-6876 1-613-591-1943	technicalsupport@controlmicrosystems.com
Europe	Mon-Fri 8am - 5:30pm CET	+31 71 579-1655	euro-support@controlmicrosystems.com
Asia Pacific	Mon-Fri 8:30am - 5:00pm AEST	+61 3 9249 9580	au-support@controlmicrosystems.com