ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-173-01—CLEARSCADA REMOTE AUTHENTICATION BYPASS

August 25, 2011

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-173-01P “ClearSCADA Remote Authentication Bypass”, on the US-CERT Portal on June 22, 2011. This web page release was delayed to allow users sufficient time to download and install this update.

Independent security researcher Jeremy Brown has identified an authentication bypass vulnerability in Control Microsystems’ ClearSCADA application. Control Microsystems has produced a new version that mitigates this vulnerability. ICS-CERT has tested the new version to validate that it is fixed.

AFFECTED PRODUCTS

The following ClearSCADA versions are affected:

- 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 the following (these SCX versions contain ClearSCADA in the bundle):

- SCX Version 67 R4.5
- SCX Version 68 R3.9

IMPACT

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

BACKGROUND

Control Microsystems, a Schneider Electric company, is a global supplier of SCADA hardware and software products.[a] The company's products are used in water and wastewater automation, natural gas and crude oil production and pipeline automation,[b] and substation automation and power applications.

ClearSCADA is an integrated SCADA host platform that includes a polling engine, real-time database, historian, web server, alarm processor, and a reporting package. The client applications function as the human-machine interface.[c] While ClearSCADA is optimized for use with Control Microsystems SCADAPack field devices, it has built-in drivers for most major third-party controllers.

Serck UK and Serck AUS sell a bundle called SCX that includes ClearSCADA.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

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.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could allow a remote attacker to view sensitive information and possibly modify functions of the server running on the affected host.

EXISTENCE OF EXPLOIT

No publicly available exploits are known to exist for this vulnerability.

DIFFICULTY

An attacker with intermediate level skills could develop code to exploit this vulnerability.

MITIGATION

Control Microsystems has corrected this vulnerability in its regular maintenance release.

Control Microsystems recommends the following to all users of ClearSCADA:

[a] http://www.clearscada.com/about-us/ website last accessed 8/23/2011

[b] http://investing.businessweek.com/research/stocks/private/snapshot.asp?privcapId=24439754 website last accessed 8/23/2011

[c] http://www.clearscada.com/product-features/product-architecture/ website last accessed 8/23/2011

- Limit server and server network access 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.

Contact the Regional Sales Manager or Control Microsystems representative for additional information. Users can also contact the factory directly at 1-888-267-2232.

ICS-CERT encourages asset owners to minimize network exposure for all control system devices. Critical devices should not directly face the Internet. Locate control system networks and remote devices behind firewalls and isolate them from the business network. When remote access is required, use secure methods such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) also provides a recommended practices section for control systems on the CSSP web page. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[d]

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

Can I edit this document to include additional information? This document may not be edited or modified in any way by recipients nor may any markings be removed. It may not be posted on public

[d] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

Web sites. All comments or questions related to this document should be directed to the ICS-CERT at ics-cert@dhs.gov.