ICS-CERT ADVISORY

ICSA-10-314-01 —MULTIPLE VULNERABILITIES IN CLEARSCADA SOFTWARE

February 1, 2011

OVERVIEW

Researchers at Digital Bond have identified multiple vulnerabilities in Control Microsystems' ClearSCADA application. The following vulnerabilities have been identified:

- Heap Overflow Vulnerability
- Cross-site Scripting Vulnerabilities
- Insecure Web Authentication.

AFFECTED PRODUCTS

The following ClearSCADA versions are affected:

- ClearSCADA 2005 (all versions)
- ClearSCADA 2007 (all versions)
- ClearSCADA 2009 (all versions).

IMPACT

Successful exploitation of the vulnerabilities reported in this Advisory requires an attacker to have a level of skill that ranges from intermediate to high depending on the specific vulnerability and desired objective. An attacker can perform a number of malicious actions including a denial of service attack on the ClearSCADA application that can have a significant impact on control systems operating in critical environments.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on the environment, architecture, and product implementation.

BACKGROUND

Control Microsystems, a Schneider Electric company, is a global supplier of SCADA hardware and software products. The company's products are used in water and wastewater automation, natural gas, crude oil production, pipeline automation, 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. ClearSCADA is optimized for use with Control Microsystems' SCADAPack field devices but also includes drivers for most major controllers.

ClearSCADA supports a variety of interfaces for communication with field devices including DNP3,

IEC 60870, and Modbus. ClearSCADA supports OPC data exchange with historians and other servers.

VULNERABILITY CHARACTERIZATION

HEAP OVERFLOW VULNERABILITY OVERVIEW

A heap-based buffer overflow vulnerability was found in the ClearSCADA application. The overflow identified is a "use after free" type heap overflow. Reliable heap corruption was discovered by sending overly long strings following a valid packet. This heap overflow can cause a denial of service condition for the ClearSCADA application, or it could be leveraged for remote code execution.

EXPLOITABILITY

An attacker with an intermediate skill level could develop code to exploit this vulnerability to cause a denial of service condition. Leveraging this heap overflow for remote code execution would be significantly more difficult.

EXISTENCE OF EXPLOIT

Currently, no known exploits are targeting this vulnerability.

INSECURE WEB AUTHENTICATION OVERVIEW

ClearSCADA provides a web interface that supports both HTTP (plain-text) and HTTPS (encrypted) for remote connections. By default, the ClearSCADA server uses HTTP; this allows anyone with access to the connection between the client and server to view authentication credentials in plain text (unsecure).

INSECURE WEB AUTHENTICATION DETAILS

EXPLOITABILITY

An attacker who can sniff a logon session can intercept credentials passed in plain text to capture usernames and passwords. The difficulty of intercepting this traffic is based on an attacker's ability to gain strategic access within the target network architecture.

EXISTENCE OF EXPLOIT

Tools are publicly available to perform network sniffing that could be used to exploit this vulnerability.

CROSS-SITE SCRIPTING VULNERABILITIES OVERVIEW

The web interface is vulnerable to reflective (nonpersistent) cross-site scripting. Using this vulnerability, an attacker could potentially inject malicious code directly into the user's browsing session. Parameters are passed back to the user without being properly sanitized.

CROSS-SITE SCRIPTING VULNERABILITIES DETAILS

EXPLOITABILITY

Successful exploit of this vulnerability requires interaction by the user making the request. Modern browsers also have protection mechanisms against such attacks that make this exploit more difficult to execute.

EXISTENCE OF EXPLOIT

Tools are publicly available that could aid in exploiting this cross-site scripting vulnerability.

MITIGATION

This Advisory does not apply to users of ClearSCADA 2010 R1.

ClearSCADA 2009 users can obtain service packs for ClearSCADA 2009 R2.3 and ClearSCADA 2009 R1.4 at this link: http://www.clearscada.com/services-support/software-updates/

ICS-CERT and Control Microsystems recommend that users upgrade ClearSCADA 2005 (all versions) and ClearSCADA 2007 (all versions) as soon as possible to the updated versions listed below.

Updated Software Versions:

- ClearSCADA 2010 R1
- ClearSCADA 2009 R2.3
- ClearSCADA 2009 R1.4.

The upgrade is free of charge with a valid Control Microsystems SCADACare support agreement.

In addition, Control Microsystems recommends the following to all ClearSCADA users:

- Disable logons on ClearSCADA non-secure ports. Locate this setting under System Configuration => WebX in the server configuration window.
- Install a WebX security certificate from a trusted authority.
- Limit access to the server and server network to only trusted networks and users.
- Upgrade the ClearSCADA server to ClearSCADA 2010 R1, or the latest service packs for ClearSCADA 2009 R2 and ClearSCADA 2009 R1, as appropriate.

Note: All three issues affect the ClearSCADA server. No action is required for ViewX clients.

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

As with all system changes, administrators should consult their control systems vendor prior to making any control system changes.

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

The Control System Security Program provides numerous recommended practices[a] for control systems on the US-CERT website. Several relevant recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*

ICS-CERT CONTACT

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

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For Control System Security Program Information and Incident Reporting: http://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.

a. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed January 12, 2010.