ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-10-070-02—AUTHENTICATION VULNERABILITY IN ROCKWELL PLC-5 AND SLC 5/0X CONTROLLERS AND ASSOCIATED RSLOGIX SOFTWARE

March 11, 2010

OVERVIEW

Rockwell Automation has identified a security vulnerability in the programming and configuration client software authentication mechanism employed by certain versions of the PLC-5 and SLC 5/0x family of programmable controllers.

AFFECTED PRODUCTS

Rockwell PLC-5 and SLC 5/0x controllers are affected, including the following catalog numbers: 1785-Lx and 1747-L5x. The programming and configuration client software, RSLogix, for these devices is also affected by this vulnerability. For a complete listing of affected products and firmware versions, please see Rockwell's Technotes.[a,b]

IMPACT

A significant number of PLC-5s and SLC 500s are installed worldwide. Successful exploitation of these vulnerabilities may expose the controller's access control password and allow unauthorized programming of the controller.

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

BACKGROUND

Rockwell PLC-5 and SLC 5/0x controllers are used worldwide in diverse process control environments. These PLCs can be used in both centralized control systems and in remote installations, including remote communication and control to enable SCADA solutions for water/waste-water treatment facilities.

[a] Rockwell Technote, http://rockwellautomation.custhelp.com/app/answers/detail/a_id/66684/kw/vulnerability/r_id/115100, website last accessed March 4, 2010

[b] Rockwell Technote, http://rockwellautomation.custhelp.com/app/answers/detail/a_id/66678/kw/vulnerability/r_id/115100, website last accessed March 4, 2010

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The following two vulnerabilities have been identified:

1. The potential exists for exposure of the product's password used to restrict unauthorized access to the controller.

   To expose the password, an attacker would need direct access to the product or the control system communication link between the controller and configuration software. The attacker could then intercept and decipher the product’s password and use it to emulate the role of the client software to gain unauthorized access to the product.

2. The potential exists for an unauthorized programming and configuration client to gain access to the product and allow changes to the product’s configuration or program.

   An attacker, with direct access to the product or the control system communication link between the controller and configuration software, could emulate the role of a trusted software client and potentially make unauthorized changes to the product.

VULNERABILITY DETAILS

EXPLOITABILITY

An attacker can exploit these vulnerabilities in order to:

1 Cause a denial of service.
2. Gain unauthorized access with elevated privileges to the product.
3. Possibly leverage these vulnerabilities in an attempt to find additional vulnerabilities elsewhere in a control system network.

EXISTENCE OF EXPLOIT

There are currently no known exploits specifically targeting these vulnerabilities.

DIFFICULTY

Research indicates that these vulnerabilities can be easily exploited by a skilled attacker; however, access to the control system network is required for successful exploitation.

MITIGATION

To help reduce the likelihood of exploitation and associated security risk, Rockwell Automation recommends the following immediate mitigation strategies (Note: multiple strategies are recommended to be employed simultaneously):

1. For PLC-5 controllers, enable and configure "Passwords and Privileges" via RSLogix 5 configuration software to restrict access to critical data and improve overall password security.
2. When applicable, upgrade product firmware to a version that includes enhanced security functionality compatible with Rockwell Automation's FactoryTalk Security services. This functionality can be enabled via RSLogix 5 or RSLogix 500 software. *(Consult Rockwell Technote*[c] *for applicable firmware versions)*
3. Use the latest version of RSLogix 5 or RSLogix 500 configuration software and enable FactoryTalk Security services.
4. Disable where possible the capability to perform remote programming and configuration of the product over a network to a controller by placing the controller's key switch into RUN mode.
5. For SLC controllers, enable static protection on all critical data table files to prevent any remote data changes to critical data.
6. Employ layered security and defense-in-depth methods in system design to restrict and control access to individual products and control networks. Refer to http://www.ab.com/networks/architectures.html for comprehensive information about implementing validated architectures designed to deliver these measures.
7. Block all traffic to the CSP, Ethernet/IP, or other CIP protocol-based devices from outside the Manufacturing Zone by restricting or blocking access to TCP and UDP Port 2222 and Port 44818 using appropriate security technology (e.g., a firewall, UTM devices, or other security device).
8. Restrict physical and electronic access to automation products, networks, and systems to only those individuals authorized to make changes to control system equipment.
9. Frequently change the product’s password and obsolete previously used passwords to reduce exposure to threat from a product password becoming known.

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

[c] Rockwell Technote, http://rockwellautomation.custhelp.com/app/answers/detail/a_id/66678/kw/vulnerability/r_id/115100, website last accessed January 12, 2010

[d] Control System Security Program (CSSP) Recommended Practices, http://csrp.inl.gov/Recommended_Practices.html, website last accessed January 12, 2010.

CONTACT ICS-CERT:

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