ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-12-342-01A—ROCKWELL ALLEN-BRADLEY MICROLOGIX, SLC 500, AND PLC-5 FAULT GENERATION VULNERABILITY

UPDATE A

December 11, 2012

OVERVIEW

Independent researcher Matthew Luallen of CYBATI has identified a fault generation vulnerability that can cause a denial of service (DoS) in the Rockwell Automation Allen-Bradley MicroLogix, SLC 500, and PLC-5 controller. Rockwell has released a notification[a] that includes mitigation strategies for this vulnerability.

This vulnerability could be exploited remotely.

--------- Begin Update A Part 1 of 5 --------

Rockwell has not developed a patch that resolves this vulnerability. They continue to evaluate whether a patch will be created for this issue.

--------- End Update A Part 1 of 5 ----------

AFFECTED PRODUCTS

Rockwell Automation reports that the vulnerabilities affect the following versions of Allen-Bradley devices:

- MicroLogix 1100 controller,[b]
- MicroLogix 1200 controller,
- MicroLogix 1400 controller,
- MicroLogix 1500 controller,
- SLC 500 controller platform,[c] and

a. 511407 - MicroLogix, SLC 500 and PLC-5 Controller Vulnerability, https://rockwellautomation.custhelp.com/app/answers/detail/a_id/511407

b. MicroLogix Systems, http://ab.rockwellautomation.com/programmable-controllers/micrologix-systems.

c. SLC 500 Control System, http://ab.rockwellautomation.com/programmable-controllers/slc-500.

This product is provided subject only to the Notification Section as indicated here: http://www.us-cert.gov/privacy/

- PLC-5 controller platform.[d]

IMPACT

--------- Begin Update A Part 2 of 5 --------

This vulnerability affects the availability of the device and connected devices.

A successful attack will cause the controller to cease its logic execution and enter a fault state. Recovery from this fault state requires the controller's operating mode selector to be switched via direct physical interaction.

--------- End Update A Part 2 of 5 ----------

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 operational environment, architecture, and product implementation.

BACKGROUND

Rockwell Automation provides industrial automation control and information products worldwide, across a wide range of industries.

--------- Begin Update A Part 3 of 5 --------

The affected products, MicroLogix, SLC500, and PLC5 are programmable logic controllers (PLC). According to Rockwell Automation, these products are deployed across several sectors including agriculture and food, water, chemical, manufacturing and others. According to Rockwell's Web site, these products are used in Germany, Czech Republic, France, Poland, Denmark, Hungary, Italy and other countries in Europe, as well as the United States, Korea, China, Japan, and Latin American countries.

--------- End Update A Part 3 of 5 ----------

d. PLC-5 Control System, http://ab.rockwellautomation.com/programmable-controllers/plc-5.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

MODIFICATION OF ASSUMED-IMMUTABLE DATA[e]

When certain configuration parameters are not enabled, the affected devices are susceptible to a remote attack. To exploit the vulnerability, the attacker sends specially crafted messages that change specific bits in status files. This creates a device fault, which in turn causes a DoS.

--------- Begin Update A Part 4 of 5 --------

Attackers sending malicious packets to Port 2222 TCP/UDP and Port 44818 TCP/UDP will cause the device fault. An attack will be successful regardless of controller's mode switch setting. Physical interaction is required to recover the device.

--------- End Update A Part 4 of 5 ----------

CVE-2012-4690[f] has been assigned to this vulnerability. A CVSS v2 base score of 8.5 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:P/A:C).[g]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

e. CWE-471: Modification of Assumed Immutable Data, http://cwe.mitre.org/data/definitions/471.html, Web site last accessed December 11, 2012.

f. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4690 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

g. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:P/A:C, Web site last visited December 11, 2012.

MITIGATION

Rockwell Automation continues to assess the feasibility of enhancing security features of the MicroLogix platform to directly address or mitigate associated risk from this vulnerability. Due to technical limitations of the platform, the viability of altering the platform's operation or adding specific product controls to mitigate risk continues to be explored.

Rockwell Automation recommends[a] the following mitigation strategies to help reduce the likelihood of compromise and the associated security risk. When possible, multiple strategies should be employed simultaneously.

- If possible, change the controller's settings to the nonvulnerable state:
  - SLC-500: Set the Status file to "Static"
  - PLC-5: Enable the Passwords and Privileges feature.
- 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.
- Employ firewalls with ingress/egress filtering, intrusion detection/prevention systems, and validate all configurations. Evaluate firewall configurations to ensure other appropriate inbound and outbound traffic is blocked.
- Block all traffic to the EtherNet/IP or other CIP protocol based devices from outside the Manufacturing Zone by restricting or blocking access to both TCP and UDP Port# 2222 and Port 44818 using appropriate security technology (e.g., a firewall, UTM devices, or other security appliance).
- Restrict physical and electronic access to automation products, networks and systems to only those individuals authorized to be in contact with control system equipment.

--------- Begin Update A Part 5 of 5 --------

There is currently no patch for this vulnerability. Rockwell has provided the above security mitigations to assist as they continue to evaluate whether a patch will be created for this issue.

For more information about this vulnerability or other problems with a Rockwell device, please contact the Rockwell Automation Support Center.[h]

--------- End Update A Part 5 of 5 ----------

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet or be directly exposed to areas of less trust.
- 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 with confidentiality, integrity and two-factor authentication controls (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[i] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01A—Cyber Intrusion Mitigation Strategies,[j] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

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 CONTACT

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

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585

h. Rockwell Automation Support Center, https://rockwellautomation.custhelp.com/

i. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed December 11, 2012.

j. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed December 11, 2012.

For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

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.

May 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 ICS-CERT at ics-cert@hq.dhs.gov.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.