ICS-CERT ADVISORY

ICSA-11-273-03—ROCKWELL RSLOGIX DENIAL-OF-SERVICE VULNERABILITY

September 30, 2011

OVERVIEW

This advisory is a follow-up to the Alert titled "ICS-ALERT-11-256-05A – Rockwell RSLogix Overflow Vulnerability" that was published September 13, 2011, on the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) web page.

ICS-CERT is aware of a public report of a denial-of-service vulnerability in Rockwell Automation's RSLogix application. Rockwell has produced a patch that mitigates this vulnerability in FactoryTalk Services Platform, Versions CPR 9 SR4 and CPR 9 SR3. Patches for prior versions of FactoryTalk Services Platform and RSLogix 5000 are currently under development. ICS-CERT has not tested this patch to validate that it resolves this vulnerability.

AFFECTED PRODUCTS

According to Rockwell Automation, the following products are affected:

- RSLogix 5000 software Versions V17, V18, and V19
- All FactoryTalk-branded software of specific Versions CPR9 and CPR9-SR1 through SR4.

IMPACT

Successful exploitation of this vulnerability could result in a denial-of-service.

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.

RSLogix 5000 is a programming suite used to develop interfaces within the control system environment.

The FactoryTalk Services Platform is a collection of production and performance management systems.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

A Read Access violation can occur when a specially crafted packet is sent to open ports running the software. The open TCP ports are as follows:

- 1330
- 1331
- 1332
- 4241
- 4242
- 4445
- 4446
- 5241
- 6543
- 9111
- 60093
- 49281

CVE-2011-3489 has been assigned to this vulnerability in the National Vulnerability Database (NVD).[a] A CVSS base score of 5.0 has been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to target this vulnerability.

DIFFICULTY

An attacker with a low skill level can create the denial-of-service.

MITIGATION

Rockwell Automation recommends that concerned customers using FactoryTalk Services Platform Version CPR 9 SR4 apply patch AID 456854[b] and CPR 9 SR3 apply patch AID 457488.[c] Customers using prior versions of FactoryTalk Services Platform and RSLogix should apply those patches as they become available. ICS-CERT will update this advisory accordingly as these patches are released.

For more information, refer to Rockwell Automation Security Advisory KB 456144. http://rockwellautomation.custhelp.com/app/answers/detail/a_id/456144.

a. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3489, website last accessed September 30, 2011.
b. http://rockwellautomation.custhelp.com/app/answers/detail/a_id/456854, website last accessed September 30, 2011.
c. http://rockwellautomation.custhelp.com/app/answers/detail/a_id/457488, website last accessed September 30, 2011.

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.
- 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.

The Control Systems Security Program (CSSP) also provides a section for control system security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.[d] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

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:

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

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is provided when prior coordination has occurred with either the vendor, ICS-CERT, or other coordinating entity. 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 (ICSs) and the public at avoidable risk.

d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed September 30, 2011.