ICS-CERT ADVISORY

ICSA-12-088-01—ROCKWELL AUTOMATION FACTORYTALK RNADIAGRECEIVER DOS VULNERABILITIES

March 28, 2012

OVERVIEW

This advisory is a follow-up to ICS-CERT Alert "ICS-ALERT-12-017-01—ROCKWELL AUTOMATION FACTORYTALK RNADIAGRECEIVER"[a] that was published January 17, 2012, on the ICS-CERT web page.

Independent researcher Luigi Auriemma identified two vulnerabilities that may result in a denial-of-service (DoS) condition in the Rockwell Automation FactoryTalk (FT) application. These vulnerabilities were reported, along with proof-of-concept code, without coordination with ICS-CERT, the vendor, or other coordinating entity. The two vulnerabilities include an unexpected return value and a read access violation.

ICS-CERT has coordinated these vulnerabilities with Rockwell Automation who developed a patch that resolves these vulnerabilities.

AFFECTED PRODUCTS

According to Rockwell Automation's Security Taskforce, the following Allen-Bradley products are affected by these vulnerabilities:

- RSLogix 5000 (versions 17, 18, 19, 20)
- Factory Talk (CPR9 up to and including CPR9 SR5)
  - FT Directory
  - FT Alarms & Events
  - FT View SE
  - FT Diagnostics
  - FT Live Data
  - FT Server Health.

a. http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-12-017-01.pdf, date last accessed March 27, 2012

IMPACT

Successful exploitation of this vulnerability may result in a DoS condition.

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 their operational environment, architecture, and product implementation.

BACKGROUND

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

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

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

UNEXPECTED RETURN VALUE[b]

An unexpected return value can be generated by a specially crafted packet which can cause the Rockwell Automation FactoryTalk RNADiagReceiver service listening on Port 4445/TCP to stop processing packets. This vulnerability may lead to a DoS condition.

CVE-2012-0221[c] has been assigned to this vulnerability.

READ ACCESS VIOLATION[d]

A read access violation vulnerability exists in Rockwell Automation's FactoryTalk platform. A specially crafted packet can be sent to the RNADiagReceiver service listening on Port 4445/TCP resulting in a possible DoS condition.

CVE-2012-0222[e] has been assigned to this vulnerability.

b. CWE, http://cwe.mitre.org/data/definitions/389.html, CWE-389: Error Conditions, Return Values, Status Codes. This website last accessed March 27, 2012.
c. CWE, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0221, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
d. CWE, http://cwe.mitre.org/data/definitions/125.html, CWE-125: Out-of-bounds Read. This website last accessed March 27, 2012.
e. NIST, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0222, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known that target these vulnerabilities.

DIFFICULTY

An attacker with a low skill level may be able to exploit these vulnerabilities.

MITIGATION

Rockwell has developed a security update to address these vulnerabilities. To download and install the update please refer to Rockwell's Advisory at http://rockwellautomation.custhelp.com/app/answers/detail/a_id/469937.

For more information on security with Rockwell Automation products, please refer to Rockwell's Security Advisory Index at http://rockwellautomation.custhelp.com/app/answers/detail/a_id/54102.

In addition to applying the above patch, Rockwell Automation recommends customers configure firewalls to block the following TCP ports to prevent traversal of RNA messages into and out of the ICS system:

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

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 systems 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.*[f] 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.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams*[g] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[h] for more information on social engineering attacks.

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 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.

f. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed March 27, 2012.
g. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed March 27, 2012.
h. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed March 27, 2012.