ICS-CERT ADVISORY

ICSA-11-175-01— ROCKWELL AUTOMATION FACTORYTALK DIAGNOSTIC VIEWER MEMORY CORRUPTION VULNERABILITY

June 24, 2011

OVERVIEW

Independent security researchers Billy Rios and Terry McCorkle have coordinated with ICS-CERT on a memory corruption vulnerability that affects Rockwell's Automation FactoryTalk Diagnostics Viewer product.

By using a specially crafted FactoryTalk Diagnostics Viewer configuration file, an attacker could possibly cause a memory corruption that allows the execution of arbitrary code.

According to Rockwell Automation, this issue has been resolved in later versions of the FactoryTalk Diagnostics Viewer, starting with V2.30.00 (CPR9 SR3). ICS-CERT has not validated this update.

AFFECTED PRODUCTS

According to Rockwell Automation, these vulnerabilities affect Versions 2.10.x (SPR9 SR2) and earlier.

IMPACT

A successful exploitation of this vulnerability could result in the execution of arbitrary code.

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

The FactoryTalk Diagnostics Viewer is part of the FactoryTalk Services Platform and collects, stores, and provides access to activity, status, warning, and error messages generated by products during installation, configuration, and operation.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The memory corruption vulnerability could allow an attacker to execute arbitrary code using a specially crafted FactoryTalk Diagnostics Viewer configuration file (.ftd extension).

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is not remotely exploitable. The exploit can only be triggered when the specially crafted file is executed locally by a vulnerable version of FactoryTalk Diagnostics Viewer.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability requires moderate skill. Social engineering is required to convince the user to accept the malformed file, decreasing the likelihood of a successful exploit.

MITIGATION

Rockwell Automation recommends that concerned customers upgrade the FactoryTalk Diagnostics Viewer to the latest version. Because FactoryTalk Diagnostics Viewer is not available as a standalone installation, customers must upgrade the FactoryTalk Services Platform product to FactoryTalk Diagnostics Viewer (CPR9 SR3) or greater.

Rockwell Automation also recommends its customers review the Rockwell Automation Software Product Compatibility Matrix[a] to ensure they understand the dependencies and compatibilities that may arise as a result of upgrading this product.

For more information, refer to Rockwell Automation Security Advisory KB#448424 - http://rockwellautomation.custhelp.com/app/answers/detail/a_id/448424

a. Rockwell Automation Software Product Compatibility Matrix, http://rockwellautomation.custhelp.com/app/answers/detail/a_id/42682, last accessed June 22, 2011.

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*[b] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[c] for more information on social engineering attacks.

ICS-CERT encourages asset owners to 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.

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 reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

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 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.

b. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website accessed June 22, 2010.
c. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website accessed June 22, 2011.
d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html