ICS-CERT ADVISORY

ICSA-11-161-01—ROCKWELL AUTOMATION RSLINX CLASSIC EDS HARDWARE INSTALLATION TOOL BUFFER OVERFLOW

June 10, 2011

OVERVIEW

ICS-CERT has received a report from Michael Orlando of CERT Coordination Center (CERT/CC) identifying a vulnerability in Rockwell Automation Electronic Data Sheet (EDS) Hardware Installation Tool. This tool is bundled with RSLinx Classic for normal distribution. The install tool exhibits a buffer overflow vulnerability when parsing improperly formatted EDS files. This vulnerability is likely exploitable and could allow remote code execution, though that would require significant user interaction. Rockwell Automation has released a patch that has been verified by CERT/CC.

AFFECTED PRODUCTS

EDS Hardware Installation Tool Version 1.3.0.1 and all earlier versions are affected.

IMPACT

An attacker could exploit the vulnerability by tricking a user into opening a specially crafted EDS file, causing the EDS Hardware Installation Tool to crash, which would lead to possible execution of arbitrary code.

ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their environment, architecture, and product implementation. Critical infrastructure organizations are encouraged to use the information contained in this advisory to strengthen network defense and examine their own networks for possible compromise.

BACKGROUND

Rockwell Automation provides industrial automation control and information products worldwide, across a wide range of industries. RSLinx provides connectivity to plant floor devices for Rockwell software applications. To register a device on the network, product-specific information must be supplied via an EDS file. The RSLinx Hardware Installation Tool parses the EDS file containing the hardware's specifications.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

An attacker that alters a required EDS file and then uses it in the EDS Hardware Installation Tool could cause the tool to crash, allowing execution of arbitrary code. The subsequent stack-based buffer overflow[a] usually results from an excessively recursive function call and is usually outside the scope of a program's implicit security policy. When the consequence is arbitrary code execution, this can often be used to subvert any other security service.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is likely exploitable; however, it is not possible without user interaction. An attacker cannot initiate the exploit from a remote machine. The exploit is only triggered when a local user runs the vulnerable application and loads the malformed EDS file.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability would be difficult. Social engineering is required to convince the user to accept the malformed EDS file. Additional user interaction is needed to load the malformed file. This decreases the likelihood of a successful exploit.

MITIGATION

Rockwell Automation recommends concerned customers take the following immediate steps to mitigate risk associated with this vulnerability.

1. Restrict physical access to the computer
2. Establish policies and procedures such that only authorized individuals have administrative rights on the computer
3. Obtain product EDS files from trusted sources (e.g., product vendor)
4. Download and apply the Rockwell Automation issued Patch Aid 276774, available from the Rockwell Automation Support Center (requires an account logon for access): http://rockwellautomation.custhelp.com/app/answers/detail/a_id/276774.

a Mitre, http://cwe.mitre.org/data/definitions/121.html, website last visited June 09, 2011

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.[b]

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

b. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html
c. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed June 9, 2011.
d. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed June 9, 2011.