ICS-CERT ADVISORY

ICSA-10-070-01A-UPDATE—ROCKWELL AUTOMATION RSLINX CLASSIC EDS HARDWARE INSTALLATION TOOL BUFFER OVERFLOW

May 3, 2010

OVERVIEW

A buffer overflow vulnerability exists in the Rockwell Automation RSLinx Classic EDS Hardware Installation Tool (RSHWare.exe). This vulnerability is likely exploitable; however, significant user interaction would be required.

AFFECTED PRODUCTS

EDS Hardware Installation Tool Version 1.0.5.1 and earlier.

IMPACT

The CVSS impact subscore for this vulnerability, as calculated by ICS-CERT, is high (10) because successfully exploiting this vulnerability would allow an attacker to run arbitrary code on the target machine. However, the exploitability subscore is low (3.2) because of the difficulty of exploiting this vulnerability.

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.

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 Electronic Data Sheet (EDS) file. The RSLinx Hardware Installation Tool parses the EDS file containing the hardware's specifications.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

On February 9, 2010, a security researcher posted a blog entry regarding a buffer overflow vulnerability in an EDS file installation tool, later found to be the Rockwell Automation EDS Hardware Installation Tool (RSHWare.exe). ICS-CERT has verified that the vulnerability exists in RSLinx Classic Version 2.41.00 (RSHWare.exe Version 1.0.4.0).

VULNERABILITY DETAILS

COMMON VULNERABILITY SCORING SYSTEM (CVSS) SCORE[a]

Overall CVSS Score: 6.2

- CVSS Base Score: 6.9
  - *Impact Subscore: 10*
  - *Exploitability Subscore: 3.4*
- CVSS Temporal Score: 6.2
- CVSS Environmental Score: Organization Defined

Shorthand CVSS Scoring Notation:
AV:L/AC:M/Au:N/C:C/I:C/A:C/E:POC/RL:U/RC:C

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

There are currently no known exploits specifically targeting 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.

a. As calculated by ICS-CERT using the NVD CVSS Scoring system—http://nvd.nist.gov/cvss.cfm, website last accessed March 5, 2010

MITIGATION

Rockwell Automation (http://rockwellautomation.custhelp.com/app/answers/detail/a_id/67272) recommends customers take the following 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).

Rockwell Automation will modify the EDS Hardware Installation Tool to properly handle EDS files and will release the modified version as a patch by May 2010. This modified version will be included in all future releases of RSLinx Classic starting with Version 2.57.

***** BEGIN UPDATE *****

Rockwell Automation has issued a software patch for the EDS Hardware Installation Tool that addresses this buffer overflow vulnerability. When applied, the patch replaces the RSEds.dll file with the modified Version 4.0.1.157. Future releases of RSLinx Classic, starting with Version 2.57, will include this modified version of the RSEds.dll.

Rockwell has also updated Technote 67272[b] to include instructions for how to obtain and apply the patch.

***** END UPDATE *****

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.

The Control System Security Program also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[e]

b. Rockwell Automation, http://rockwellautomation.custhelp.com/app/answers/detail/a_id/67272, website last accessed May 3, 2010.

c. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf., website last accessed March 5, 2010

d. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed March 4, 2010.

e. Control System Security Program (CSSP) Recommended Practices, http://csrp.inl.gov/Recommended_Practices.html, website last accessed January 12, 2010.

CONTACT ICS-CERT:

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 Control System Security Program 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.

Can 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 the ICS-CERT at ics-cert@dhs.gov.