ICS-CERT ADVISORY

ICSA-13-014-01—SIEMENS SIMATIC RF MANAGER ACTIVEX BUFFER OVERFLOW

January 14, 2012

OVERVIEW

This advisory provides mitigation details for a vulnerability that impacts the Siemens SIMATIC RF Manager.

Siemens has identified a buffer overflow vulnerability in the ActiveX component of the SIMATIC RF Manager. Siemens has produced a patch that mitigates this vulnerability. Successful exploitation of this vulnerability could lead to possible remote code execution or a denial of service.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The following Siemens products are affected:

- SIMATIC RF Manager 2008, and
- SIMATIC RF Manager Basic v3.0 and lower (as distributed with RF670R and RF 640R).

IMPACT

The RF Manager uses ActiveX and this component can also be accessed within Internet browsers. A user would have to visit a malicious Web site on the system in which RF Manager is installed to exploit the vulnerability. By exploiting this vulnerability, an attacker could execute remote code and could cause a denial of service of the RF Manager. This could impact the setup of systems in the critical manufacturing, health and healthcare, power generation and distribution, food and beverage, and chemical industries.

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

Products in the Siemens SIMATIC RF Manager family manage connected radio frequency identification (RFID) readers to SIMATIC S7 controllers. This includes collecting supplied data, and compressing this data for enterprise systems, such as the Enterprise Resource Management (ERP) layer and Manufacturing Execution Systems (MES) layer. ERP and MES are widely used in industrial environments such as critical manufacturing, health and healthcare, power generation and distribution, food and beverage, and chemical industries worldwide.

Siemens is a German-based company that maintains offices in several countries around the world.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

BUFFER OVERFLOW[a]

The SIMATIC RF Manager uses an ActiveX component. This component is also shared with other programs, such as Internet browsers. If a user has installed the SIMATIC RF Manager's ActiveX applications on the system and visits a malicious Web site, code within the ActiveX components can be executed, causing a buffer overflow. This could allow an attacker to execute arbitrary code in the browser context and possibly take control of the system.

CVE-2013-0656[b] has been assigned to this vulnerability. Siemens has assigned a CVSS v2 base score of 6.8; the CVSS vector string is (AV:N/AC:M/Au:N/C:P/I:P/A:P).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

a. CWE-119: Heap-based Buffer Overflow, http://cwe.mitre.org/data/definitions/119.html, Web site last accessed January, 14, 2013.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-0656, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:M/Au:N/C:P/I:P/A:P), Web site last visited January, 14, 2013

DIFFICULTY

Exploiting this vulnerability could be difficult. Social engineering is required to convince the user to visit a malicious Web site using the system containing the SIMATIC RF Manager. This decreases the likelihood of a successful exploit.

MITIGATION

Siemens has released a Siemens Security Advisory[d] (SSA-099471: Buffer Overflow in SIMATIC RF Manager) that details this vulnerability and provides mitigations. Siemens has released a software patch that mitigates the vulnerability. Siemens requests that users contact Siemens' customer support to obtain the patch.[e]

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.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT 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.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01A—Cyber Intrusion Mitigation Strategies,[g] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

d. Siemens SSA-099471, http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-099741.pdf, Web site last accessed January 14, 2013.

e. Siemens' Customer Support, http://support.automation.siemens.com/WW/view/en/66829257, Web site last visited January 14, 2013.

f. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed January 14, 2013.

g. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed January 14, 2013.

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.

Previous Recommendations can be used as needed (otherwise, delete this text). List other products that are specific to the topic (i.e., phishing mitigations):

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 email messages.
2. Refer to Recognizing and Avoiding Email Scams[h] for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing Attacks[i] for more information on social engineering attacks.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

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

h. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, Web site last accessed January 14, 2013.
i. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, Web site last accessed January 14, 2013.

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.