ICS-CERT ADVISORY

ICSA-11-361-01— SIEMENS AUTOMATION LICENSE MANAGER MULTIPLE VULNERABILITIES

December 27, 2011

OVERVIEW

This Advisory is a follow-up to the original Alert titled "ICS-ALERT-11-332-01**A**—Siemens Automation License Manager Multiple vulnerabilities" that was published December 02, 2011, on the ICS-CERT web page.

ICS-CERT is aware of publicly disclosed reports of four vulnerabilities in Siemens Automation License Manager (ALM) application. These vulnerabilities include:

- Buffer overflow
- Exception
- Null pointer
- Improper input validation.

Independent researcher Luigi Auriemma publicly disclosed four vulnerabilities along with proof-of-concept (PoC) exploit code without coordination from Siemens, ICS-CERT, or any other coordinating entity known to ICS-CERT.

Siemens has confirmed these vulnerabilities and has released a patch to address the issue. ICS-CERT has not validated the patch.

AFFECTED PRODUCTS

Siemens software products that include ALM Version 4.0 to 5.1+SP1+Upd1 are affected by the buffer overflow, exception, and null pointer vulnerabilities.

Siemens software products that include ALM Version 2.0 to 5.1+SP1+Upd2 are affected by the improper input validation vulnerability.

IMPACT

Successful exploitation of these vulnerabilities could result in denial of service, write to memory, file corruption, or remote code execution.

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

Siemens is a German multinational company headquartered in Munich with activities in the fields of industry, energy, and healthcare.

Siemens ALM is an application that centrally manages licenses for various Siemens products. The products contact ALM either locally or remotely to verify their license. This software is used in many industries including: food and beverage, water and wastewater, oil and gas, and chemical.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

BUFFER OVERFLOW

ALM does not check the length of a field used in various commands sent to the server via TCP port 4410. This vulnerability may lead to remote code execution.

CVE-2011-4529[a] has been assigned to this vulnerability. A CVSS V2 base score of 8.3 has also been calculated by Siemens.

EXCEPTION

In multiple cases, ALM does not check the length of fields used in various commands sent to the server via TCP Port 4410. These vulnerabilities cause exceptions within the application, which cause the application to quit and enable denial-of-service attacks.

CVE-2011-4530[b] has been assigned to this vulnerability. A CVSS V2 base score of 6.1 has also been calculated by Siemens.

a. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4529, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4530, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

NULL POINTER

ALM does not check the content of a field used for command sent to the server via TCP port 4410. This vulnerability causes a null pointer dereference, which cause the application to quit and enables a Denial-of-Service attack.

CVE-2011-4531[c] has been assigned to this vulnerability. A CVSS v2 base score of 6.1 has also been calculated by Siemens.

IMPROPER INPUT VALIDATION

ALM uses an ActiveX control in its graphical user interface. This control exports a method that allows saving a file to the local hard disk. A malicious web site that the user accesses with Internet Explorer may delete the content of any file on the system that the user is allowed to write to, and create new files.

CVE-2011-4532[d] has been assigned to this vulnerability. A CVSS v2 base score of 8.8 has also been calculated by Siemens.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are remotely exploitable.

EXISTENCE OF EXPLOIT

Publicly released PoC code exists for these vulnerabilities.

DIFFICULTY

Crafting a working exploit for these vulnerabilities would require a moderate skill level. Social engineering is required to exploit the improper input validation vulnerability.

MITIGATION

Siemens has released a patch to its customers to address these vulnerabilities. Customers of vulnerable versions of Siemens ALM should deploy the Siemens patch available at:
http://support.automation.siemens.com/WW/view/en/114358

c. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4531, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
d. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4532, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

For more information, please see Siemens' Security Advisory announcement available at: http://www.siemens.com/cert/advisories/

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

e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed December 27, 2011.

f. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed December 27, 2011.

g. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed December 27, 2011.

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.