



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-12-349-01—SIEMENS AUTOMATION LICENSE MANAGER UNCONTROLLED RESOURCE CONSUMPTION

December 14, 2012

OVERVIEW

This advisory provides mitigation details for a vulnerability that impacts the Siemens Automation License Manager (ALM).

Siemens ProductCERT has identified an uncontrolled resource consumption vulnerability^a in the Siemens ALM, which is used for license management by various Siemens software products. Siemens has produced a software update that fully resolves this vulnerability. Exploitation of this vulnerability would allow loss of availability of the system.

AFFECTED PRODUCTS

All Siemens software products that include ALM version between 4.0 and 5.2 are affected. The following Siemens product families are affected:

- SIMATIC (e.g., STEP 7)
- SIMATIC HMI (e.g., WinCC, WinCC flexible)
- SIMATIC PCS 7
- SIMOTION (e.g., Scout)
- SIMATIC NET
- SINAMICS (e.g., Starter)
- SIMOCODE.

IMPACT

Attackers could exploit the vulnerability to cause memory leakage within the software. This exploit could eventually lead to a crash of the application. The DoS of the ALM could lead to a DoS of associated devices that use the ALM to verify active licenses.

a. SSA-783261, http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-783261.pdf, Web site last accessed December 14, 2012.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

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 multinational company headquartered in Munich, Germany. Siemens develops products mainly in the energy, transportation, and healthcare sectors.

ALM centrally manages licenses for various Siemens software products. The products contact ALM either locally or remotely to verify their license using a proprietary protocol. To enable this license verification, ALM listens on Port 4410/TCP by default. These products are deployed across several sectors including energy, healthcare, and others worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

UNCONTROLLED RESOURCE CONSUMPTION^b

An attacker can send maliciously crafted packets to Port 4410/TCP, which will cause a memory leakage and uncontrolled resource consumption, leading to a DoS.

CVE-2012-4691^c has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).^d

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

b. CWE, <http://cwe.mitre.org/data/definitions/400.html>, CWE-400: Uncontrolled Resource Consumption (“Resource Exhaustion”), Web site last accessed December 14, 2012.

c. NVD, <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4691>, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

d. CVSS Calculator, [http://nvd.nist.gov/cvss.cfm?version=2&vector=\(AV:N/AC:L/Au:N/C:N/I:N/A:C\)](http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:N/I:N/A:C)), Web site last visited December 14, 2012.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

MITIGATION

Siemens has provided an update^e that resolves this vulnerability. The update can be applied to all versions of ALM starting with version 4.0. Siemens recommends that asset owners and operators can contact Siemens customer support^f to acquire the update.

Siemens recommends blocking traffic to Port 4410/TCP from external and remote connections.

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.^g 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,^h that is available for download from the ICS-CERT Web page (www.ics-cert.org).

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.

e. SSA-783261, http://www.siemens.com/corporate-technology/pool/de/forschungsfelder/siemens_security_advisory_ssa-783261.pdf, Web site last accessed December 14, 2012.

f. Siemens Customer Support, msp.support.de@siemens.com

g. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed December 14, 2012.

h. Cyber Intrusion Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01A.pdf, Web site last accessed December 14, 2012.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

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 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.