ICS-CERT ALERT

ICS-ALERT-11-332-01A—SIEMENS AUTOMATION LICENSE MANAGER MULTIPLE VULNERABILITIES

December 02, 2011

ALERT

SUMMARY

This Alert Update is a follow-up to the original ICS-CERT Alert titled "ICS-ALERT-11-332-01—Siemens Automatic License Manager" that was published November 28, 2011 on the ICS-CERT web page.

ICS-CERT is aware of a public report of four vulnerabilities with proof-of-concept (PoC) exploit code affecting the Siemens Automation License Manager (ALM). According to this report, the vulnerabilities are remotely exploitable. This report was released by Luigi Auriemma without coordination with Siemens, ICS-CERT, or any other coordinating entity known to ICS-CERT.

ICS-CERT has coordinated the report with Siemens, who is working to confirm the report and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

--------- Begin Update A Part 1 of 1 --------

The ALM is a component of Siemens industrial software and is necessary for licensing Siemens supervisory control and data acquisition (SCADA), human-machine interface (HMI), and engineering software.

The report includes vulnerability details and PoC exploit code for four vulnerabilities. Siemens has analyzed the vulnerability report and offered the following vulnerability characterization information.

Vulnerability Type	Exploitability	Impact
Buffer Overflow	Remote	Denial of Service (DoS) / Possible Remote Code Execution
Exception	Remote	DoS
NULL Pointer	Remote	DoS
Improper Input Validation	Remote	Write access to file system allowing arbitrary file deletion

--------- End Update A Part 1 of 1 ----------

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

MITIGATION

ICS-CERT is currently coordinating with Siemens to identify mitigations.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[a]
- Locate control system networks and devices behind firewalls, and isolate them from the business network.
- If remote access is required, employ secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

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 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*.[b]

Organizations that observe 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 CONTACT

ICS-CERT Operations Center
1-877-776-7585
ics-cert@dhs.gov

For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats 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 declines attribution.

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed December 01, 2011.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed December 01, 2011.

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.