ICS-CERT ADVISORY

ICSA-11-244-01—SIEMENS WINCC FLEXIBLE RUNTIME ADVANCED LOADER HEAP OVERFLOW

September 06, 2011

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-244-01P on the US-CERT secure Portal on September 01, 2011. This web page release was delayed to allow users sufficient time to download and install the update.

Independent security researchers Billy Rios and Terry McCorkle have reported a memory corruption vulnerability in the WinCC Runtime Advanced Loader, which is a component of both Siemens SIMATIC WinCC flexible and TIA Portal.

ICS-CERT has coordinated with Siemens and the researchers. Siemens has not issued a patch to address this vulnerability. However, Siemens has provided recommended mitigations to assist asset owners with protecting their systems.

AFFECTED PRODUCTS

According to Siemens, the following software packages are vulnerable:

- Siemens SIMATIC WinCC flexible Runtime
- Siemens SIMATIC WinCC (TIA Portal) Runtime Advanced.

IMPACT

Successful exploitation of this vulnerability may result in the ability to execute arbitrary code on the targeted human-machine interface system.

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

Siemens SIMATIC WinCC flexible and WinCC (TIA Portal) Runtime Advanced is a software package used for visualization and machine or small system operations. These products run on standard PCs or on Siemens panel PCs. This software is used in many industries, including: food and beverage, water and wastewater, oil and gas, and chemical.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The runtime loader does not properly sanitize inputs on 2308/TCP. A specially crafted packet can result in memory corruption, leading to a denial of service. Remote code execution may also be possible.

MITRE[a] has assigned number CVE-2011-3321 to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable if a system has been configured with the WinCC flexible Runtime Loader and WinCC (TIA Portal) Runtime Advanced Loader enabled.

EXISTENCE OF EXPLOIT

No publicly available exploits are known to specifically target this vulnerability.

DIFFICULTY

This vulnerability requires a basic skill level to exploit.

MITIGATION

Siemens currently has no plans to patch this vulnerability. The WinCC flexible Runtime Loader and WinCC (TIA Portal) Runtime Advanced Loader feature is disabled by default and is only used when updating firmware. Siemens has updated the product documentation to advise users to disable this feature except when it is actively being used.

Siemens strongly recommends that their customers protect control systems according to Control Systems Security Program (CSSP) recommended security practices[b] and that they configure the environment according to the Siemens operational guidelines.[c]

Siemens Security Advisory can be found here:
http://support.automation.siemens.com/WW/view/de/29054992.

Users should monitor network traffic to 2308/TCP and control traffic to the WinCC system.

[a] http://cve.mitre.org/cve/, website last accessed September 06, 2011.

[b] CSSP Recommended Practices:http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed September 06, 2011.

[c] Siemens, PCS7 Security Concept Recommendations and Notes: http://support.automation.siemens.com/WW/view/en/22229786, website last accessed September 06, 2011.

ICS-CERT encourages asset owners to minimize network exposure for all control system devices. Specifically:

- 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 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.

CSSP also provides a recommended practices section for control systems on the CSSP web page. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[d]

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.

[d] CSSP Recommended Practice: *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*, http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf, website last accessed September 06, 2011.