ICS-CERT ADVISORY

ICSA-11-175-02—SIEMENS SIMATIC WINCC EXPLOITABLE CRASHES

July 01, 2011

OVERVIEW

ICS-CERT Advisory ICSA-11-175-02P was originally released to the US-CERT Portal on June 24, 2011. This web page release was delayed to allow users sufficient time to download and install the update.

ICS-CERT has received a report from independent security researchers Billy Rios and Terry McCorkle concerning exploitable crashes in the Siemens SIMATIC WinCC SCADA product. Specially crafted files can cause memory corruption or pointer issues, which can cause the system to crash.

ICS-CERT has coordinated with the researchers and Siemens to assist with releasing an update that successfully mitigates these vulnerabilities. The researchers have validated that this update successfully mitigates these vulnerabilities.

AFFECTED PRODUCTS

Siemens reports that this vulnerability affects the following versions of WinCC:

- ProTool 6.0 SP3 (has been phased-out)
- WinCC flexible 2004 (has been phased-out)
- WinCC flexible 2005 (has been phased-out)
- WinCC flexible 2005 SP1
- WinCC flexible 2007
- WinCC flexible 2008
- WinCC flexible 2008 SP1
- WinCC flexible 2008 SP2.

IMPACT

Successful exploitation of this vulnerability results in a memory corruption, which could be used to execute arbitrary code.

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

The Siemens SIMATIC WinCC is a software package used to develop network-based plant visualization systems. WinCC can be configured as a stand-alone SCADA system or as the human-machine interface component of a larger SIMATIC system. WinCC is used in many industries including: food and beverage, water and wastewater, oil and gas, and chemical.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The following vulnerabilities have been identified.

1. Memory Corruption: client side exploit that allows arbitrary code execution.
2. DoS / Null pointer issues: client side exploit.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is likely exploitable, but not without user interaction. An attacker cannot initiate the exploit from a remote machine. The exploit can be triggered only when a local user runs the vulnerable application and loads the carefully crafted exploit file.

EXISTENCE OF EXPLOIT

No publicly known exploits specifically target this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability would require moderate skill. Social engineering is required to convince the user to accept the malformed file. Additional user interaction is needed to load the malformed file, decreasing the likelihood of a successful exploit.

MITIGATION

Siemens has released an update mitigating this vulnerability. This update is available at the following location on their website:

http://support.automation.siemens.com/WW/llisapi.dll?func=cslib.csinfo&lang=en&objid=50182361

ICS-CERT recommends that system operators thoroughly test new releases of software before installing them on critical production systems.

ICS-CERT encourages asset owners to 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.

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. 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 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.*[a]

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

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.

a. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website accessed June 23, 2011.

b. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf., website accessed June 23, 2011.

c. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website accessed June 23, 2011.