ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-017-02— SIELCO SISTEMI WINLOG STACK OVERFLOW

January 17, 2011

OVERVIEW

Independent researcher Luigi Auriemma reported a stack overflow vulnerability in Version 2.07.00 of Sielco Sistemi’s WinLog Lite and Winlog Pro HMI software.

Sielco Sistemi has developed an update (Version 2.07.01) to address this vulnerability. The researcher has verified that the update is effective in correcting this vulnerability.

AFFECTED PRODUCTS

This vulnerability affects all versions of Sielco Sistemi’s WinLog Lite and WinLog Pro prior to Version 2.07. 00.

IMPACT

Winlog is used in building automation, monitoring systems, and food production in 16 countries around the world. Sielco Sistemi is based in Italy.

While a successful exploit of this vulnerability could lead to arbitrary code execution, the 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

Winlog is a SCADA/HMI software package for the supervision of industrial and civil plants. It can connect to PLCs, controllers, motor drives, and I/O modules.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The Winlog system can act as a server by enabling the "Run TCP/IP server" option. The server listens on TCP port 46823. A specially crafted packet from a remote attacker can cause a stack overflow possibly allowing an attacker to execute arbitrary code.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is exploitable from a remote machine.

EXISTENCE OF EXPLOIT

This exploit code and vulnerability details are publicly available.

DIFFICULTY

A high level of skill is needed to exploit this vulnerability.

MITIGATION

ICS-CERT recommends that users of Sielco Sistemi's Winlog system take the following mitigation steps:

- Update Winlog Lite and WinLog Pro to the latest Version (2.07.01).

  www.sielcosistemi.com/download/WinlogLite_Setup.exe

  www.sielcosistemi.com/download/Winlog_Setup_SF.exe

  For additional information, customers can contact Sielco Sistemi's support at:

  http://www.sielcosistemi.com/en/support/

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet. Control system networks and remote devices should be located behind firewalls and be isolated from the business network. If remote access is required, secure methods such as Virtual Private Networks (VPNs) should be used.

Organizations should follow their established internal procedures if any suspected malicious activity is observed and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

The Control System Security Program 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.*[1]

[1] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html.

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 Control System Security Program 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.