ICS-CERT ADVISORY

ICSA-11-298-01**A**—SIELCO SYSTEMI WINLOG BUFFER OVERFLOW

UPDATE A

December 27, 2011

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-298-01P on the US-CERT secure portal on October 25, 2011. This web page release was delayed to allow users time to download and install the update.

Independent researcher Paul Davis has identified a buffer overflow vulnerability in Sielco Sistemi Winlog application. Sielco Sistemi has produced a new release that mitigates this vulnerability. Mr. Davis has indicated to ICS-CERT that he has tested the new release and validated that it resolves the vulnerability.

AFFECTED PRODUCTS

The following Sielco Sistemi products are affected:

- Winlog Lite versions older than Version 2.07.09
- Winlog PRO versions older than Version 2.07.09.

IMPACT

Successful exploitation of this vulnerability could lead to a program crash or arbitrary code execution.

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

Sielco Sistemi is an Italy-based company that creates supervisory control and data acquisition (SCADA)/human-machine interface (HMI) software and hardware products.

Winlog Lite is a demo version of the Winlog PRO SCADA/HMI system. According to Sielco Sistemi, Winlog PRO is deployed across several sectors including manufacturing, public utilities, telecommunications, and others. Sielco Sistemi products are deployed in about 16 countries around the world.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

In the affected versions, Winlog does not properly sanitize the inputs from project files. Invalid information in certain fields can overwrite memory locations, which causes the program to crash and could be used to execute arbitrary code.

CVE-2011-4037[a] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is not remotely exploitable and cannot be exploited without user interaction. The exploit is only triggered when a local user runs the vulnerable application and loads the malformed file.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability would be difficult. 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

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

Sielco Sistemi advises users to download the new Winlog release, from their website www.sielcosistemi.com and follow download instructions found there.

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

Sielco Sistemi plans to send a message to all customers telling of the vulnerability and the new release that mitigates it. The new release can be installed in the same manner as the previous release.

ICS-CERT encourages asset owners to take the following 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.

a. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4037 , NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

- 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.

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*.[b] 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.

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

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

b. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed December 27, 2011.
c. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed December 27, 2011.
d. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed December 27, 2011.

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.