ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-12-277-01— SIELCO SISTEMI WINLOG LITE SEH OVERWRITE VULNERABILITY

October 3, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report of Structured Exception Handler (SEH) overwrite vulnerability with proof-of-concept (PoC) exploit code affecting Sielco Sistemi WinLog Lite SCADA HMI, a supervisory control and data acquisition/human-machine interface (SCADA/HMI) product. According to this report, the vulnerability is exploitable by overwriting the SEH to allow insertion and execution of shell-code. This report was released by independent security researcher “FaryadR” (a.k.a. Ciph3r) on the Web site packetstormsecurity.org[a] without coordination with either the vendor or ICS-CERT.

ICS-CERT has notified the affected vendor of the report and has asked the vendor to confirm the vulnerability 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.

The report included vulnerability details and PoC exploit code for the following vulnerability:

Vulnerability Type	Remotely Exploitable	Impact
Structured Exception Handler	No	Possible Code Execution

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

AFFECTED PRODUCTS

Sielco Sistemi—WinLog Lite SCADA HMI, ver. 2.06.17

Sielco Sistemi is based in Italy with numerous sales and support offices worldwide providing multiple SCADA/HMI solutions.

[a] Website, http://packetstormsecurity.org/files/116013/Winlog-Lite-SCADA-HMI-System-2.06.17-SEH-Overwrite.html, Web site last accessed October 3, 2012.

MITIGATION

ICS-CERT is currently coordinating with the vendor 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.[b]
- 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.

ICS-CERT also provides a recommended practices section for control systems on the US-CERT Web site. Several recommended practices are available for reading or download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[c]

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
Email: ics-cert@dhs.gov

For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

[b] ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, Web site last accessed October 3, 2012.

[c] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed October 3, 2012.

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 notifies ICS-CERT that they 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.