ICS-CERT ALERT

ICS-ALERT-12-179-01—SIELCO SISTEMI WINLOG MULTIPLE VULNERABILITIES

June 27, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report of multiple vulnerabilities with proof-of-concept (PoC) exploit code affecting Sielco Sistemi Winlog Version 2.07.14, a supervisory control and data acquisition/human-machine interface (SCADA/HMI) product. According to this report, the vulnerabilities can be exploited remotely by sending specially crafted requests to TCP/46824. The public report was released by independent security researcher Luigi Auriemma without coordination with either the vendor or ICS-CERT.

ICS-CERT has notified Sielco of the report and has asked Sielco to confirm the vulnerabilities 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 vulnerabilities.

Vulnerability Type	Remotely Exploitable	Impact
Multiple Buffer Overflows[a]	Yes	Possible Remote Code Execution
Directory Traversal (Improper Access Control)[b]	Yes	Information Leakage
Improper Access of Indexable Resource[c]	Yes	Possible Remote Code Execution

a. http://cwe.mitre.org/data/definitions/121.html, Web site last accessed June 27, 2012
b. http://cwe.mitre.org/data/definitions/284.html, Web site last accessed June 27, 2012
c. http://cwe.mitre.org/data/definitions/118.html, Web site last accessed June 27, 2012

Vulnerability Type	Remotely Exploitable	Impact
Write-What-Where Condition[d]	Yes	Possible Remote Code Execution

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT (ics-cert@hq.dhs.gov).

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.

MITIGATION

ICS-CERT is currently coordinating with the vendor and security researcher 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.[e]
- 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.

The Control Systems Security Program (CSSP) 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.[f] 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.

d. http://cwe.mitre.org/data/definitions/123.html, Web site last accessed June 27, 2012

e. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, Web site last accessed June 27, 2012.

f. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed June 27, 2012.

ICS-CERT CONTACT

ICS-CERT Operations Center
1-877-776-7585
Email: ics-cert@dhs.gov

For CSSP Information and Incident Reporting: www.ics-cert.org

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.