ICS-CERT ALERT

ICS-ALERT-12-284-01—SINAPSI ESOLAR LIGHT PHOTOVOLTAIC SYSTEM MONITOR MULTIPLE VULNERABILITIES

October 10, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report of multiple vulnerabilities with proof-of-concept (PoC) exploit code[a] affecting the Sinapsi eSolar Light Photovoltaic System Monitor, a supervisory control and data acquisition (SCADA) monitoring product. According to the vendor's website,[b] the company is based in Italy. The product has also been also sold as the Enerpoint eSolar Light, Schneider Electric Ezylog Photovoltaic Management Server, Gavazzi Eos-Box, and Astrid Green Power Guardian.

According to researchers Roberto Paleari and Ivan Speziale, the vulnerabilities are exploitable remotely by authenticating to the service using hard-coded credentials. Exploitation of these vulnerabilities would allow attackers to remotely connect to the server and executing remote code, possibly affecting the availability and integrity of the device. This report was released without coordination with either the vendor or ICS-CERT.

ICS-CERT has notified the affected vendor of this report and has asked the vendor to confirm the vulnerability and identify mitigations. ICS-CERT is unaware of any validated mitigations or workarounds at this time. This product is used in the Energy Sector. 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.

a. Multiple vulnerabilities in Ezylog photovoltaic management server, http://www.exploit-db.com/exploits/21273/, Web site last accessed October 10, 2012.

b. Sinapsi eSolar Light, http://www.sinapsitech.it/default.asp?active_page_id=81, Web site last accessed October 10, 2012.

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

Vulnerability Type	Remotely Exploitable	Impact
Hard-coded Credentials	Yes	Unauthorized Authentication
SQL Injection	Yes	Information Leakage
Command Execution	Yes	Remote Code Execution
Broken Session Enforcement	Yes	Unauthorized Authentication

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

MITIGATION

ICS-CERT is currently coordinating with the vendor and security researchers to identify mitigations.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should perform the following.

- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[c]
- 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.[d]

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

d. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed October 10, 2012.

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/.

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.