ICS-CERT ALERT

ICS-ALERT-11-266-01—SUNWAY FORCE CONTROL VULNERABILITY

September 23, 2011

ALERT

SUMMARY

ICS-CERT is aware of publicly available exploit code targeting multiple vulnerabilities in Sunway Force Control Version 6.1. The vulnerabilities include stack overflows, directory traversal and arbitrary file reading, and various denials of service vulnerabilities.

ICS-CERT is coordinating with Sunway on this report and will provide additional information as it becomes available.

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

BACKGROUND

Beijing-based Sunway ForceControl Technology Co. provides SCADA human-machine interface applications for a variety of industries. Sunway's products are deployed primarily in China. According to the Sunway website,[a] Sunway products are also deployed in Europe, the Americas, Asia, and Africa. Sunway products are deployed across a wide variety of industries including petroleum, petrochemical, defense, railways, coal, energy, pharmaceutical, telecommunications, water, and manufacturing.

MITIGATION

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.

[a] http://www.sunwayland.com.cn, website last accessed August 26, 2011.

[b] ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, accessed September 23, 2011.

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.*[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
ICS-CERT@DHS.GOV

For Control Systems Security Program (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.

[c] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, accessed September 23, 2011.