ICS-CERT ALERT

ICS-ALERT-11-238-01A—SUNWAY FORCE CONTROL SCADA 6.1 SEH VULNERABILITY

UPDATE A

August 31, 2011

ALERT

SUMMARY

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

On August 26, 2011, ICS-CERT became aware of publicly available exploit code targeting a vulnerability in Sunway Force Control SCADA Version 6.1. The vulnerability results from inadequate bounds checking, which could allow execution of arbitrary code.

Initial ICS-CERT analysis of this public exploit indicates that the exploit is likely targeting a previously disclosed and patched vulnerability that was coordinated by ICS-CERT and security researcher Dillon Beresford, as reported in ICS-CERT Advisory ICSA-11-167-01.[a] ICS-CERT has reached out to Sunway, the author of the exploit code, and to Mr. Beresford in order to confirm this analysis.

Concerned customers using affected versions of Sunway Force Control are encouraged to follow the mitigation recommendations provided in ICS-CERT Advisory ICSA-11-167-01.[a]

ICS-CERT will provide additional information as it becomes available.

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

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,[b] 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.

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.

a. ICS-CERT Advisory "ICSA-11-167-01—Heap Overflow Vulnerabilities in Sunway ForceControl and pNetPower," http://www.us-cert.gov/control_systems/pdf/ICSA-11-167-01.pdf, website last accessed August 31, 2011.
b. http://www.sunwayland.com.cn, website last accessed August 26, 2011.

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.