ICS-CERT ALERT

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

August 26, 2011

ALERT

SUMMARY

ICS-CERT is aware of a structured exception handler (SEH) overwrite vulnerability in Sunway Force Control SCADA Version 6.1. Boundary errors that occur during various functions can cause heap-based or stack-based buffer overflows, which in turn may allow execution of arbitrary code. ICS-CERT is currently coordinating with the vendor to validate and mitigate this vulnerability. Additional information will be published as it becomes available.

Beijing-based Sunway ForceControl Technology Co. provides SCADA HMI applications for a variety of industries. Sunway's products are deployed primarily in China. According to the Sunway website,[a] the 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.

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.

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