ICS-CERT ALERT

ICS–ALERT-11-080-03—MULTIPLE VULNERABILITIES IN 7-TECHNOLOGIES IGSS

March 21, 2011

ALERT

SUMMARY

An independent researcher has published eight vulnerabilities with proof of concept (POC) code in the 7-Technologies (7T) IGSS Supervisory Control and Data Acquisition (SCADA) product. IGSSdataServer listens on 12401/TCP and is reported to be vulnerable to the following:

- Directory traversal (remotely exploitable)
- Stack overflows (multiple, all remotely exploitable)
- Possible remote code execution.

Another server is running on 12397/TCP and is reported to be vulnerable to remote code execution of arbitrary executables stored on the local file system.

MITIGATION

ICS-CERT recommends that users minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[a] 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).

ICS-CERT is currently coordinating with the vendor and security researcher to identify additional mitigations. ICS-CERT will provide additional information as it becomes available.

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 reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, accessed January 17, 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.*[b]

BACKGROUND

- 7T is based in Denmark and creates monitoring and control systems that are primarily used in Europe and South Asia in the wastewater, water supply, and marine industries. IGSS is an Human-Machine Interface (HMI) application used to control and monitor Programmable Logic Controllers (PLCs) in industrial processes.
- According to the IGSS website, IGSS has been installed in over 28,000 industrial plants in 50 countries worldwide. It is deployed in multiple sectors including energy, manufacturing, oil and gas, and water.

ICS-CERT CONTACT

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

ICS-CERT Operations Center
1-877-776-7585

www.ics-cert.org
ICS-CERT@DHS.GOV

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.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html