ICS-CERT ALERT

ICS–ALERT-11-080-02—MULTIPLE VULNERABILITIES IN ICONICS GENESIS (32 & 64)

March 21, 2011

ALERT

SUMMARY

An independent researcher has published 13 vulnerabilities with proof of concept (POC) code for Iconics Genesis32 (all versions prior to and including Version 9.21) and Genesis64 (all versions prior to and including Version 10.51) Supervisory Control and Data Acquisition (SCADA) products. Multiple vulnerabilities have been reported that affect services on 38080/TCP:

- Multiple integer overflow (remotely exploitable)
- Double-free memory corruption (remotely exploitable).

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.

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).

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.

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]*

---

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, accessed January 17, 2011.

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

BACKGROUND

ICONICS is based in the US that provides automation solutions to several sectors worldwide. ICONICS maintains several offices around the world including in the US, UK, Netherlands, Italy, India, Germany, France, Czech Republic, China, and Australia. Sectors serviced by ICONICS include water and wastewater, building automation, manufacturing, food and beverage, government infrastructure, oil and gas, pharmaceutical, and energy.

The GENESIS automation suite provides a web-enabled Human-Machine Interface (HMI).

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.