ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-355-01—7-TECHNOLOGIES IGSS BUFFER OVERFLOW

December 21, 2011

OVERVIEW

Security researcher Celil Unuver (SignalSEC LLC[a]) has identified a buffer overflow vulnerability in the 7-Technologies (7T) Interactive Graphical SCADA System (IGSS) product. Successful exploitation of this vulnerability could result in a denial of service (DoS) or the execution of arbitrary code.

ICS-CERT has coordinated this vulnerability report with 7T and they have produced a patch that resolves this vulnerability. The researcher has confirmed that the patch fully resolves the reported vulnerability.

AFFECTED PRODUCTS

The following 7T Interactive Graphical SCADA System versions are affected:

- Versions 9.0.0.11355 and prior.

IMPACT

Successful exploitation of this vulnerability may allow an attacker to cause a DoS or to execute arbitrary code.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

7T, based in Denmark, creates monitoring and control systems that are primarily used in the United States, Europe, and South Asia. According to the 7T website,[b] IGSS has been deployed in over 28,000 industrial plants in 50 countries worldwide.

7T Interactive Graphical SCADA System software is used to control and monitor programmable logic controllers in industrial processes across multiple sectors including energy, manufacturing, oil and gas, and water.

[a] SignalSEC LLC, www.signalsec.com, website last accessed December 21, 2011.

[b] 7-Technologies, www.7t.dk, website last accessed December 20, 2011.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

An attacker could exploit this buffer overflow vulnerability by sending specially crafted packets to either Port 12399/TCP or Port 12397/TCP.

CVE-2011-4537[c] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill level can create the DoS whereas it would require a more skilled attacker to execute arbitrary code.

MITIGATION

7T has developed a patch to address this vulnerability and has provided the following options to customers for updating their systems:

1. In the IGSSMaster application, select the menu item “Information and Support” and click “Update IGSS Software.” This will automatically download and install the updated module. This is the preferred method for updating the IGSS installation when the host computer has Internet access.

2. Access the update either by using the direct link or the instructions below:
   Direct link: http://www.7t.dk/igss/igssupdates/v90/progupdatesv90.zip

   Instructions: Browse to the 7T IGSS website (www.igss.com). From the “Download” menu select the “Licensed Versions” option. From this page, select the Version 9 “Program updates (General)” to download a ZIP file containing all current updates for IGSS Version 9. Once the ZIP file (progupdatesv90.zip) has downloaded, manually unpack the ZIP file, and copy the entire contents to the \IGSS\ directory within the IGSS installation folder on the end user’s computer.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

[c] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4537. NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

The Control Systems Security Program (CSSP) also provides a section for control system security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[d] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams* [e] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[f] for more information on social engineering attacks.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

E-mail: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed December 21, 2011.

e. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed December 21, 2011.

f. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed December 21, 2011.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.