ICS-CERT ADVISORY

ICSA-11-335-01—7-TECHNOLOGIES IGSS DATA SERVER BUFFER OVERFLOW

December 20, 2011

OVERVIEW

ICS-CERT originally released advisory "ICSA-11-335-01P - 7-Technologies Data Server Denial of Service" in the US-CERT secure portal on December 01, 2011. This web page release was delayed to allow users time to download and install the update.

Security researcher UCQ from the Cyber Defense Institute, Inc.[a] has identified a buffer overflow vulnerability in the 7-Technologies (7T) IGSS Data Server application.

ICS-CERT has coordinated with 7T, which has produced a patch to resolve this vulnerability. The Cyber Defense Institute, Inc. has tested the patch and confirmed that it resolves the reported vulnerability.

AFFECTED PRODUCTS

Version 9.0.0.11200 of 7T IGSS Data Server is affected.

IMPACT

Successful exploitation of this vulnerability can allow an attacker to execute a remote denial of service (DoS) against the 7T data server on the targeted host computer, resulting in adverse application conditions.

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 used primarily 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.

The 7T IGSS human-machine interface (HMI) is used to control and monitor programmable logic controllers (PLCs) in industrial processes across multiple sectors including energy, manufacturing, oil and gas, and water.

a. http://www.cyberdefense.jp/en/, website last accessed December 27, 2011.
b. 7-Technologies, www.7t.dk, website last accessed December 20, 2011.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

This vulnerability can be exploited by sending a specially crafted packet to Port 12401/TCP. A successful exploit will cause a buffer overflow that can result in a remote DoS against the 7T Data Server application on the targeted host.

CVE-2011-4050[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 moderate skill level can exploit this vulnerability.

MITIGATION

7T has developed a patch to address this vulnerability and has provided the following options to customers who wish to update 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.

c. http://web nvd nist.gov/view/vuln/detail?vulnId=CVE-2011-4050, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

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

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind a properly configured firewall, 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.

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.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter declines attribution. 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.

d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed November 30, 2011.