ICS-CERT ADVISORY

ICSA-11-018-02—IGSS 8 ODBC SERVER REMOTE HEAP CORRUPTION

February 8, 2011

OVERVIEW

ICS-CERT has received a report from independent security researcher Jeremy Brown that a remote heap corruption vulnerability exists in IGSS (Interactive Graphical SCADA System) Version 8 from 7-Technologies (7T). 7T has verified the vulnerability and has developed a patch.

AFFECTED PRODUCTS

This vulnerability affects only IGSS Versions 8 and 9. Users can contact 7T for additional information.[a]

IMPACT

According to 7T, this vulnerability is more likely to be exploited for a denial of service (DoS); however, arbitrary code execution may be possible.

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 HMI (Human-Machine Interface) application used to control and monitor PLCs (Programmable Logic Controllers) 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.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

An attacker can exploit the vulnerability by sending a specially crafted packet to the server. The exploit can crash the server (DoS) or possibly allow the attacker to execute arbitrary code.

a. 7-T, http://www.igss.com/

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is exploitable from a remote machine by sending a specially crafted packet to the targeted server's listening port (20222/TCP).

EXISTENCE OF EXPLOIT

No publicly available exploits are known to exist for this vulnerability.

DIFFICULTY

Consistent exploit code is unlikely. An attacker would require at least an intermediate skill level to exploit this vulnerability.

MITIGATION

7T has created a patch for this vulnerability. ICS-CERT recommends that users of IGSS take the following mitigation steps:

Download and install the latest patch, available at the 7T website: http://www.igss.com/download/licensed-versions.aspx.

Alternately, current users can use the "update" feature from within the application.

Users should minimize network exposure for all control system devices. Critical devices should not directly face the Internet. Control system networks and remote devices should be located behind firewalls and be isolated from the business network. If remote access is required, ICS-CERT recommends the use of secure methods, such as Virtual Private Networks (VPNs).

Organizations should follow their established internal procedures if any suspected malicious activity is observed and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed 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]

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

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 Control System Security Program 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.