ICS-CERT ADVISORY

ICSA-11-189-01—7-TECHNOLOGIES IGSS ODBC REMOTE MEMORY CORRUPTION

July 08, 2011

OVERVIEW

ICS-CERT has become aware of a memory corruption vulnerability that has been coordinated with 7-Technologies (7T) by the VUPEN Vulnerability Research Team[a]. This vulnerability affects the Interactive Graphical SCADA System (IGSS) supervisory control and data acquisition (SCADA) human-machine interface (HMI) application. This vulnerability is remotely exploitable.

7T has created a patch that fully resolves this vulnerability. VUPEN has confirmed that the patch resolves the vulnerability.

AFFECTED PRODUCTS

This vulnerability affects all 7T Interactive Graphical SCADA System (IGSS) versions prior to 9.0.0.11143.

IMPACT

Successful exploitation of the reported vulnerabilities can allow an attacker to perform a number of malicious actions including denial of service (DoS) and arbitrary code execution. These actions can result in adverse application conditions and ultimately impact the process environment in which the SCADA system is deployed.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on the 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 IGSS HMI is used to control and monitor programmable logic controllers in industrial processes across multiple sectors including energy, manufacturing, oil and gas, and water.

a. http://www.vupen.com, website last accessed July 7, 2011.
b. 7-Technologies, www.7t.dk, website last accessed July 7, 2011.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The vulnerability is caused by a memory corruption error[c] in the Open Database Connectivity (ODBC) component when processing packets sent to port 20222/TCP, which could result in an invalid structure being used. This can lead to an exploitable condition.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability can be remotely exploited by sending specially crafted code to the vulnerable ODBC service. If exploited, this vulnerability could allow the attacker to execute a malicious payload.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

These vulnerabilities require advanced skills to exploit.

MITIGATION

ICS-CERT recommends that customers of 7T IGSS software take the following mitigation steps:

- Upgrade to the latest version of IGSS

  The latest version is available at: http://www.igss.com/download/licensed-versions.aspx (current users of 7T IGSS can use the "update" feature from within the application).
- 7T recommends placing the control system behind a properly configured firewall.

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

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]

c. MITRE, http://cwe.mitre.org/data/definitions/119.html, last accessed July 7, 2011.
d. 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 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.