ICS-CERT ADVISORY

ICSA-11-119-01—7-TECHNOLOGIES IGSS ODBC REMOTE STACK OVERFLOW

April 29, 2011

OVERVIEW

Security researcher James Burton of Insomnia Security has released details of a remote stack overflow vulnerability affecting 7-Technologies (7T) Interactive Graphical SCADA System (IGSS). This vulnerability exists in the IGSS Open Database Connectivity (ODBC) service running on Port 22202/TCP by default.

ICS-CERT has confirmed that Insomnia Security and 7T coordinated this vulnerability prior to public release of this report. 7T has issued an update addressing this vulnerability. ICS-CERT has received confirmation that Insomnia Security has validated the effectiveness of 7T's update in resolving the reported vulnerability.

AFFECTED PRODUCTS

This vulnerability affects 7T IGSS Version 9 and all earlier versions.

IMPACT

Successful exploitation of the reported vulnerability allows an attacker to cause a denial of service. According to Insomnia Security, this vulnerability introduces the possibility of remote code execution.

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

7T IGSS is a human-machine interface application that is used to control and monitor programmable logic controllers in industrial processes across multiple sectors, including energy, manufacturing, oil and gas, and water.

a. 7-Technolgoies, www.7t.dk

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

This stack overflow vulnerability affects the ODBC service that runs on Port 22202/TCP by default. If provided with data in excess of the size allocated for the stack, the ODBC service will experience a denial of service.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is exploitable from a remote machine by sending specially crafted data to the vulnerable ODBC service. If exploited, this vulnerability allows an attacker to cause a denial of service and possibly allows execution of arbitrary code.

EXISTENCE OF EXPLOIT

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

DIFFICULTY

An attacker would require at least an intermediate skill level to exploit this vulnerability.

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 or 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.

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 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 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]

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.

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