ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-132-01A—7-TECHNOLOGIES IGSS DENIAL OF SERVICE

UPDATE A

June 06, 2011

OVERVIEW

This Advisory updates the previously released "ICSA-11-132-01—7-Technologies IGSS Denial of Service," advisory available at: http://www.us-cert.gov/control_systems/pdf/ICSA-11-132-01.pdf by providing additional details on affected products, patch validation status, and the download links for patches.

ICS-CERT has become aware of multiple denial-of-service (DoS) vulnerabilities in the 7-Technologies (7T) Interactive Graphical SCADA System (IGSS) supervisory control and data acquisition (SCADA) human-machine interface (HMI) application. All vulnerabilities are remotely exploitable.

7T has developed patches that resolve the reported vulnerabilities in the affected versions.

--------- Begin Update A Part 1 of 3 ----------

ICS-CERT and independent researcher Joel Langill have validated the patches.

--------- End Update A Part 1 of 3 ----------

AFFECTED PRODUCTS

--------- Begin Update A Part 2 of 3 ----------

The vulnerabilities do not affect 7T IGSS SCADA HMI Version 6.

The vulnerabilities affect 7T IGSS SCADA HMI Version 7 prior to Revision 10033.

The vulnerabilities affect 7T IGSS SCADA HMI Version 8 prior to Revision 11102.

The vulnerabilities affect 7T IGSS SCADA HMI Version 9 prior to Revision 11143.

--------- End Update A Part 2 of 3 ----------

IMPACT

Successful exploitation of the reported vulnerabilities can allow an attacker to perform a remote DoS attack against the 7T data server. This action can result in adverse application conditions and ultimately impact the production environment on which the SCADA system is used.

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,[a] 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 manufacturing, energy (oil and gas), and water.

VULNERABILITY CHARACTERIZATION

DENIAL OF SERVICE VULNERABILITY OVERVIEW

The DoS vulnerability occurs in the IGSSdataServer service on Port 12401/TCP and in the dc.exe service on Port 12397/TCP.

STACK-BASED BUFFER OVERFLOW VULNERABILITY DETAILS

EXPLOITABILITY

The DoS vulnerabilities reported can be remotely exploited by sending specially crafted packets to the vulnerable IGSSdataServer service or to the dc.exe service.

EXISTENCE OF EXPLOIT

Exploit code is publicly available for these vulnerabilities.

DIFFICULTY

These vulnerabilities require moderate skills to exploit.

[a] 7-Technologies, www.7t.dk, website last accessed June 02, 2011.

MITIGATION

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

--------- Begin Update A Part 3 of 3 ----------

Download and run the “IGSS Update” to install the corresponding version patch on the system:

- Version 7 http://www.7t.dk/igss/igssupdates/v70/progupdatesv70.zip
- Version 8 http://www.7t.dk/igss/igssupdates/v80/progupdatesv80.zip
- Version 9 http://www.7t.dk/igss/igssupdates/v90/progupdatesv90.zip.

--------- End Update A Part 3 of 3 ----------

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.[b] Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[c]

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.

[b] CSSP Home Page, http://www.us-cert.gov/control_systems/index.html

[c] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html#nogo