# ICS-CERT ADVISORY

## ICSA-11-126-01—7-TECHNOLOGIES IGSS MULTIPLE VULNERABILITIES

May 06, 2011

## OVERVIEW

An independent researcher has identified eight vulnerabilities in 7-Technologies (7T) IGSS SCADA human-machine interface (HMI) application. Each of the identified vulnerabilities includes proof-of-concept (PoC) exploit code. The researcher identified the following vulnerability types:

- Stack-based buffer overflows
- Path traversal
- String formatting
- Local arbitrary code execution (dc.exe).

Seven of these vulnerabilities occur in IGSSdataServer service on Port 12401/TCP. The eighth vulnerability is identified in the Data Collection application (dc.exe) on Port 12397/TCP. Both vulnerable services run as part of the IGSS application suite. The IGSS Data Server is responsible for data transmission between the IGSS server and the operator stations. All vulnerabilities are remotely exploitable and can allow denial of service, path traversal, and arbitrary code execution.

After these original eight vulnerabilities were identified, Joel Langill of SCADAhacker[a] discovered and coordinated with ICS-CERT a ninth vulnerability. This new vulnerability is directly leveraged off one of the original vulnerabilities, specifically local arbitrary code execution affecting the Data Collection application (dc.exe) on Port 12397/TCP. An attacker could exploit this additional vulnerability to conduct simultaneous directory traversal and arbitrary programs execution on the host machine.

7T has developed a patch that resolves the reported vulnerabilities. ICS-CERT has validated the patch.

## AFFECTED PRODUCTS

The vulnerabilities affect 7T IGSS SCADA HMI prior to Version 9.0.0.11083.

## IMPACT

Successful exploitation of the reported vulnerabilities can allow an attacker to perform a number of malicious actions including denial of service, path traversal, and arbitrary code execution. These actions can result in adverse application conditions and ultimately impact the production environment on which the SCADA system is used.

a. Joel Langill, http://scadahacker.com/, website accessed May 06, 2011.

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.

# VULNERABILITY CHARACTERIZATION

## STACK-BASED BUFFER OVERFLOW VULNERABILITY OVERVIEW

Five of the reported vulnerabilities are categorized as stack-based buffer overflows.[c] Each of these five vulnerabilities occurs in the IGSSdataServer service on Port 12401/TCP. These stack-based buffer overflow vulnerabilities can be exploited by sending specially crafted code to the vulnerable IGSSdataServer service on Port 12401/TCP.

## STACK-BASED BUFFER OVERFLOW VULNERABILITY DETAILS

### EXPLOITABILITY

The five stack-based buffer overflow vulnerabilities reported can be remotely exploited by sending specially crafted code to the vulnerable IGSSdataServer service. If exploited, these vulnerabilities could allow the attacker to execute a malicious payload.

### EXISTENCE OF EXPLOIT

Exploit code is publicly available for each of the vulnerabilities.

### DIFFICULTY

These vulnerabilities require moderate skills to exploit.

b. 7-Technologies, www.7t.dk
c. Mitre, http://cwe.mitre.org/data/definitions/121.html

## PATH TRAVERSAL VULNERABILITY OVERVIEW

The sixth reported vulnerability, a path traversal[d] vulnerability, allows an attacker to perform a path traversal that exposes the file system structure and potentially allows an attacker to download or upload files without authorization.

## PATH TRAVERSAL VULNERABILITY DETAILS

### EXPLOITABILITY

This vulnerability is remotely exploitable by sending specially crafted code to the IGSSdataServer service.

### EXISTENCE OF EXPLOIT

Exploit code is publicly available for each of the vulnerabilities.

### DIFFICULTY

This vulnerability requires moderate skills to exploit.

## STRING FORMAT VULNERABILITY OVERVIEW

The seventh reported vulnerability involves a string format[e] that occurs in the IGSSdataServer service on Port 12401/TCP. This vulnerability can be exploited by sending specially crafted code to the vulnerable IGSSdataServer service on Port 12401/TCP.

## STRING FORMAT VULNERABILITY DETAILS

### EXPLOITABILITY

This vulnerability is remotely exploitable by sending specially crafted code to the IGSSdataServer service. If exploited, these vulnerabilities could allow the attacker to execute a malicious payload.

### EXISTENCE OF EXPLOIT

Exploit code is publicly available for each of the vulnerabilities.

### DIFFICULTY

This vulnerability requires moderate skills to exploit.

d. Miter, http://cwe.mitre.org/data/definitions/21.html
e. Miter, http://cwe.mitre.org/data/definitions/134.html

## CODE EXECUTION VULNERABILITY OVERVIEW

The eighth reported vulnerability, code-execution, affects the dc.exe service on Port 12397/TCP. This vulnerability results from the application failing to provide protection mechanisms for executing such code. This vulnerability could allow an attacker to remotely execute a malicious payload.

Joel Langill was able to leverage this vulnerability to identify the ninth vulnerability, another directory traversal situation.

## CODE EXECUTION VULNERABILITY DETAILS

### EXPLOITABILITY

This vulnerability is remotely exploitable by sending specially crafted code to the dc.exe service.

### EXISTENCE OF EXPLOIT

Exploit code is publicly available for each of the vulnerabilities.

### DIFFICULTY

This vulnerability requires moderate skills to exploit.

## MITIGATION

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

- Upgrade to the latest version and install the latest patch.

  The security patch is available for download from 7T at:
  http://www.7t.dk/igss/igssupdates/v90/progupdatesv90.zip

- Review 7T public news release about these vulnerabilities

  The 7T public news release is available at: http://www.igss.com/company/news-and-press-center/11-03-25/IGSS_%e2%80%93_ongoing_focus_on_security.aspx?News=NewsItem

- 7T recommends placing the 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 page of the US-CERT website. Several recommended practices are

available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.[f]

## 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.

f. CSSP Recommended Practices, *http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html#nogo*