ICS-CERT ADVISORY

ICSA-11-353-01—7-TECHNOLOGIES INTERACTIVE GRAPHICAL DLL HIJACKING

January 16, 2012

OVERVIEW

ICS-CERT originally released Advisory ICSA-11-353-01P on the US-CERT secure portal on December 19, 2011. This web page release was delayed to allow users time to download and install the update.

Researcher Kuang-Chun Hung of Security Research and Service Institute—Information and Communication Security Technology Center (ICST) has identified an unsafe search path vulnerability in the 7-Technologies (7T) IGSS Interactive Graphical SCADA System. 7T produced a patch that fixes this vulnerability. ICST tested this patch and verified that it fully resolves this vulnerability.

AFFECTED PRODUCTS

The following 7T Interactive Graphical SCADA System versions are affected:

- All versions prior to V9.0.0.11291.

IMPACT

Successful exploitation of this vulnerability may allow an attacker using social engineering to execute arbitrary code and gain the same privileges as the user that is currently logged into the system.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their 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 Interactive Graphical SCADA system software 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-Technologies, www.7t.dk, website last accessed January 16, 2012.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

To successfully exploit this vulnerability, an attacker would need to place a malicious DLL in the search path of an executable program.

CVE-2011-4053[b] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable but may require social engineering.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill level can execute this DLL hijack attack.

MITIGATION

7T developed a patch to address this vulnerability and provided the following options for updating their systems:

1. In the IGSSMaster application select the menu “Information and support” and click “Update IGSS Software.” This will automatically download and install the updated module. This is the preferred method for updating the IGSS installation when the host computer has Internet access.
2. Go to the www.igss.com website, select the menu item "Download => Licensed Versions" and click the link "Program updates (General)" for Version 9. This will download a .zip file containing all current updates for IGSS Version 9. Once the progupdatesv90.zip file is downloaded, manually unpack the .zip file and copy the contents to the \IGSS\ directory within the IGSS installation folder at the end-user’s computer.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.

b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4053 , NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

The Control Systems Security Program (CSSP) also provides a section for control systems 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.*[c] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

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.

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in e-mail messages
2. Refer to *Recognizing and Avoiding Email Scams*[d] for more information on avoiding e-mail scams
3. Refer to *Avoiding Social Engineering and Phishing Attacks*[e] for more information on social engineering attacks.

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.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before

c. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed January 16, 2012.
d. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed January 16, 2012.
e. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed January 16, 2012.

public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.