ICS-CERT ADVISORY

ICSA-12-025-01—7-TECHNOLOGIES AQUIS DLL HIJACKING

February 17, 2012

OVERVIEW

ICS-CERT originally released Advisory ICSA-12-025-01P on the US-CERT secure portal on January 25, 2012. This web page release was delayed to allow users time to download and install the update.

Researcher Kuang-Chun Hung of the Security Research and Service Institute–Information and Communication Security Technology Center (ICST) identified an uncontrolled search path element vulnerability, commonly referred to as DLL Hijacking, in the 7-Technologies (7T) AQUIS software.

ICS-CERT has coordinated this report with 7T, and 7T has created a patch that resolves this vulnerability. ICST has confirmed this patch fully resolves the reported vulnerability.

AFFECTED PRODUCTS

The following products and versions are affected:

- AQUIS V1.5 dated October 13, 2011, and any previous version.

IMPACT

A successful exploit of this vulnerability could lead to arbitrary 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 this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

7T, based in Denmark, creates monitoring and control systems that are used primarily in the United States, Europe, Northern Africa, and Asia. 7T AQUIS software is a water network simulation platform for improving system design and operation.

AQUIS may be in use in other parts of the world using a freely licensed version.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The 7T AQUIS software is vulnerable to DLL Hijacking.[a] An attacker may place a malicious DLL in a directory where it will be loaded before the valid DLL. An attacker must have access to the host file system to exploit this vulnerability. If exploited, this vulnerability may allow execution of arbitrary code.

CVE-2012-0224[b] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability may be exploitable from a remote machine. If exploited, this vulnerability may allow execution of arbitrary code.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker requires a moderate skill level to exploit this vulnerability.

MITIGATION

7T has developed a patch to address this vulnerability, which can be accessed here:

http://aquis.s3.amazonaws.com/AQUIS_1.5_14-12-2011.exe

Users may need to uninstall an earlier version of the application before installing this update.

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.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.

[a] CWE-427: Uncontrolled Search Path Element, http://cwe.mitre.org/data/definitions/427.html, website last accessed February 15, 2012.

[b] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0224, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

- 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 February 15, 2012.

[d] Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed February 15, 2012.

[e] National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed February 15, 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.