ICS-CERT ADVISORY

ICSA-12-122-01—WELLINTECH KINGVIEW DLL HIJACK VULNERABILITY

May 01, 2012

OVERVIEW

Independent researcher Carlos Mario Peñagos Hollman identified a DLL Hijack vulnerability in WellinTech's KingView application. WellinTech has created a patch that resolves the vulnerability. Mr. Hollman has tested the patch and verified that it resolves the vulnerability.

AFFECTED PRODUCTS

The following product and version are affected:

- WellinTech KingView 6.53

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

WellinTech is a software development company specializing in the automation and control industry based in Beijing, China, with branches in United States, Japan, Singapore, Europe, and Taiwan.

According to the WellinTech website, the KingView product is a Windows-based control, monitoring, and data collection application deployed across several industries including power, water, building automation, mining, and other sectors.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

UNCONTROLLED SEARCH PATH ELEMENT[a]

a. http://cwe.mitre.org/data/definitions/427.html , website last accessed May 01, 2012

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-2012-1819[b] has been assigned to this vulnerability.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable but may require the use of social engineering to exploit.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

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

MITIGATION

WellinTech has developed a patch to resolve this issue. The WellinTech advisory and the KingView product patch can be found here: http://en.wellintech.com/news/detail.aspx?contentid=168

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.
- 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.

b. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1819, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.
c. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed May 01, 2012.

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 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.

d. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed May 01, 2012.
e. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed May 01, 2012.