ICS-CERT ADVISORY

ICSA-11-355-02—WELLINTECH KINGVIEW HISTORYSERVER BUFFER OVERFLOW

December 21, 2011

OVERVIEW

ICS-CERT has received a report from the Zero Day Initiative (ZDI) concerning a heap-based buffer overflow vulnerability in WellinTech's Kingview HistoryServer.exe, which may allow a remote, unauthenticated attacker to execute arbitrary code. This vulnerability was reported to ZDI by independent security researcher Luigi Auriemma.

WellinTech has produced a patch that is available for download from its website.

AFFECTED PRODUCTS

The following WellinTech KingView version is affected:

- KingView V65.30.2010.18018

IMPACT

Successful exploitation of the heap overflow vulnerability could allow a remote attacker to cause the service to crash, and also may allow the execution of arbitrary code.

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. According to WellinTech, they also have branches in United States, Japan, Singapore, Europe, and Taiwan.

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

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

An attacker can exploit this vulnerability by sending a specially crafted packet to Port 777/TCP that exceeds a specified length and contains executable code.

CVE-2011-4536[a] has been assigned to this vulnerability. A CVSS V2 base score of 10 has also been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

No known exploits specifically target this vulnerability.

DIFFICULTY

An attacker would require an intermediate skill level to exploit this vulnerability.

MITIGATION

WellinTech has created a patch and instructions for installation that is available for download on its website at:

English: http://en.wellintech.com/news/detail.aspx?contentid=166
Chinese: http://www.kingview.com/news/detail.aspx?contentid=587

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

- Implement network or host-based firewall rules to limit network access to Port 777/TCP.
- 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.

a. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-4536. NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

The Control Systems Security Program (CSSP) also provides a section for control system 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.*[b] 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:

Do not click web links or open unsolicited attachments in e-mail messages

1. Refer to *Recognizing and Avoiding Email Scams*[c] for more information on avoiding e-mail scams
2. Refer to *Avoiding Social Engineering and Phishing Attacks*[d] 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.

b. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed September 21, 2011.
c. Recognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, website last accessed December 20, 2011.
d. National Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, website last accessed December 20, 2011.