ICS-CERT ADVISORY

ICSA-13-043-02—WELLINTECH KINGVIEW KINGMESS BUFFER OVERFLOW

February 12, 2013

OVERVIEW

This advisory provides mitigation details for a vulnerability that impacts the WellinTech KingView KingMess application.

Researchers Lucas Apa and Carlos Mario Penagos Hollman of IOActive have identified a buffer overflow vulnerability in WellinTech's KingView KingMess application. WellinTech produced and released a patch on November 15, 2012, that mitigates this vulnerability. The researchers have validated that this patch fixes the vulnerability. Exploitation of this vulnerability could allow loss of confidentiality and integrity.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The following KingView versions are affected:

- KingView 6.52 (kingMess.exe 65.20.2003.10300),
- KingView 6.53 (kingMess.exe 65.20.2003.10400), and
- KingView 6.55 (kingMess.exe 65.50.2011.18049).

IMPACT

Successful exploitation of this vulnerability will allow an attacker to execute arbitrary code as the running user. This vulnerability could impact multiple sectors, including power, water, and manufacturing.

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 China-based company that maintains offices in several countries around the world, including the US, Japan, Singapore, Taiwan, and Europe.

The affected product, KingView, is a Web-based SCADA application for Windows-based control, monitoring, and data collection. According to WellinTech, KingView is deployed across several sectors and is widely used in power, manufacturing, water and wastewater, building automation, mining, environmental protection, metallurgy, and others.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

MEMORY CORRUPTION BUFFER OVERFLOW[a]

The KingMess application in KingView has a memory corruption vulnerability where the application handles exception information incorrectly. An attacker could send a specially crafted packet to KingView, and the KingMess application would handle the packet incorrectly, causing a memory buffer overflow. This could allow the attacker to execute arbitrary code as the currently running user, which would affect confidentiality, integrity, and availability.

CVE-2012-4711[b] has been assigned to this vulnerability. A CVSS v2 base score of 10 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:C/I:C/A:C).[c]

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

a. CWE, http://cwe.mitre.org/data/definitions/119.html, CWE-119: Memory Corruption, Web site last accessed February 12, 2013.

b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4711 , NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

c. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C), Web site last accessed February 12, 2013.

DIFFICULTY

An attacker with a high skill level would be able to exploit this vulnerability.

MITIGATION

WellinTech recommends that all customers using KingView 6.52, 6.53, or 6.55 download the patch for their version of KingView that mitigates this vulnerability.

The following new versions are available at WellinTech's Web site[d]:

- KingView 6.55 (Chinese version),
- KingView 6.53 (Chinese version),
- KingView 6.52 (Chinese version),
- KingView 6.53 (English version), and
- KingView 6.52 (English version).

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.

ICS-CERT also provides a section for control systems security recommended practices on the US-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[e] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B—Targeted Cyber Intrusion

d. WellinTech download website, http://www.kingview.com/download/display1.aspx?id=225, Web site last accessed February 12, 2013.

e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed February 12, 2013.

Detection and Mitigation Strategies,[f] which is available for download from the ICS-CERT Web page (www.ics-cert.org).

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 CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

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.

f. Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01B.pdf, Web site last accessed February 12, 2013.