ICS-CERT ADVISORY

ICSA-12-185-01—WELLINTECH KINGVIEW AND KINGHISTORIAN MULTIPLE VULNERABILITIES

July 03, 2012

OVERVIEW

Independent researchers Carlos Mario Penagos Hollman and Dillon Beresford identified multiple vulnerabilities in WellinTech's KingView and a single vulnerability in WellinTech's KingHistorian application. These vulnerabilities are exploitable remotely. WellinTech has created a patch and the researchers have validated that the patch resolves these vulnerabilities in the KingView and KingHistorian applications.

AFFECTED PRODUCTS

The following products and versions are affected:

- WellinTech KingView 6.53, and
- WellinTech KingHistorian 3.0.

IMPACT

Successful exploitation of these vulnerabilities could lead to arbitrary code execution, information disclosure, and denial of service (DoS).

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 automation and control. WellinTech is based in Beijing, China, with branches in the United States, Japan, Singapore, Europe, and Taiwan.

According to the WellinTech Web site, 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. The KingHistorian product is a database

that can be used as a stand-alone historian; it is deployed across several industries including water and power and other sectors.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW—KINGVIEW APPLICATION

STACK-BASED BUFFER OVERFLOW[a]

By sending a specially crafted packet to Port 555/TCP, an attacker may create a stack-based buffer overflow in the KingView application. This attack may allow the execution of arbitrary code.

CVE-2012-1830[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]

HEAP-BASED BUFFER OVERFLOW[d]

By sending a specially crafted packet to Port 555/TCP, an attacker may create a heap-based buffer overflow in the KingView application. This attack may allow the execution of arbitrary code.

CVE-2012-1831[e] 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).[f]

OUT-OF-BOUNDS READ[g]

By sending a specially crafted packet to either Port 2001/TCP or Port 2001/UDP, an attacker may read from an invalid memory location in the KingView application. This attack may allow the execution of arbitrary code.

a. CWE, http://cwe.mitre.org/data/definitions/121.html , Web site last accessed July 3, 2012.
b. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1830, 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 visited July 3, 2012.
d. CWE, http://cwe.mitre.org/data/definitions/122.html , Web site last accessed July 3, 2012.
e. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1831, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
f. 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 visited July 3, 2012.
g. CWE, http://cwe.mitre.org/data/definitions/125.html , Web site last accessed July 3, 2012.

CVE-2012-1832[h] 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).[i]

PATH TRAVERSAL[j]

By sending a specially crafted GET request via HTTP on Port 8001/TCP, an attacker may access arbitrary information from the KingView application.

CVE-2012-2560[k] has been assigned to this vulnerability. A CVSS v2 base score of 5 has been assigned. The CVSS vector string is (AV:N/AC:L/Au:N/C:P/I:N/A:N).[l]

VULNERABILITY OVERVIEW—KINGHISTORIAN APPLICATION

IMPROPER RESTRICTION OF OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER[m]

By sending a specially crafted packet to Port 5678/TCP, an attacker may create an invalid pointer write in the KingHistorian application. This attack may allow the execution of arbitrary code.

CVE-2012-2559[n] 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).[o]

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are exploitable remotely.

h. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1832, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
i. 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 visited July 3, 2012.
j. CWE, http://cwe.mitre.org/data/definitions/35.html. Web site last accessed July 3, 2012.
k. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2560, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
l. http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:P/I:N/A:N). Web site last visited July 3, 2012.
m. CWE, http://cwe.mitre.org/data/definitions/119.html, Web site last accessed July 3, 2012.
n. NVD, 2560http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-2559, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.
o. 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 visited July 3, 2012.

EXISTENCE OF EXPLOIT

No known public exploits specifically target these vulnerabilities.

DIFFICULTY

An attacker requires a moderate skill level to exploit these vulnerabilities.

MITIGATION

WellinTech has developed patches to resolve these issues. The WellinTech advisory and the KingView product patch can be found here: http://www.wellintech.com/index.php/news/33-patch-for-kingview653. The WellinTech advisory and the KingHistorian product patch can be found here: http://en2.wellintech.com/products/detail.aspx?contentid=25.

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.[p] 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.

p. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed July 3, 2012.

ICS-CERT CONTACT

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

Email: ics-cert@dhs.gov
Toll Free: 1-877-776-7585
For CSSP Information and Incident Reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a very 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.