ICS-CERT ADVISORY

ICSA-11-074-01—WELLINTECH KINGVIEW ACTIVEX CONTROL

March 15, 2011

OVERVIEW

An independent security researcher reported a stack-based buffer overflow vulnerability in an ActiveX control in WellinTech KingView V6.53. The researcher has publicly released exploit code for this vulnerability. Successful exploitation of this vulnerability could allow a remote attacker to execute arbitrary code. WellinTech has released an update for the vulnerable file. ICS-CERT has confirmed the update resolves the vulnerability.

AFFECTED PRODUCTS

This vulnerability affects all language versions of WellinTech KingView V6.53.

IMPACT

Because KingView is widely used in many sectors and different applications, the 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 environment, architecture, and product implementation.

BACKGROUND

According to the WellinTech website, KingView is a human machine interface (HMI) for backend control systems operations. WellinTech KingView is widely used in power, water, building automation, mining, and other sectors, including the aerospace industry. Most WellinTech customers are located in China.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

The “ValidateUser” method in an ActiveX component for the KingView product may be called with a specially crafted argument to cause a stack-based buffer overflow. Exploitation of this vulnerability may lead to arbitrary code execution. The vulnerability is found in the file KVWebSvr.dll. All language versions of WellinTech KingView V6.53 are vulnerable, including the 6.53 (2010-12-15) patch.

VULNERABILITY DETAILS

EXPLOITABILITY

ICS-CERT analysis indicates that an attacker can create successful exploit code but would likely experience inconsistent results. This vulnerability is remotely executable.

EXISTENCE OF EXPLOIT

An exploit for this vulnerability is publicly available.

DIFFICULTY

An attacker would require a moderate skill level to exploit this vulnerability.

MITIGATION

WellinTech recommends that users of affected versions of WellinTech KingView replace the vulnerable KVWebSrv.dll with the updated file.

- The updated KVWebSrv.dll file is available from:

  http://download.kingview.com/software/kingview%20Chinese%20Version/KVWebSvr.rar

- Replace the original KVWebSrv.dll file with the updated file. By default, KVWebSrv.dll is located in the "c:\Program Files\Kingview\" directory.

ICS-CERT recommends that users minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[a] Locate control system networks and devices behind firewalls, and isolate them from the business network. If remote access is required, employ secure methods such as Virtual Private Networks (VPNs).

Organizations should follow their established internal procedures if any suspected malicious activity is observed and report their findings to ICS-CERT for tracking and correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

The Control System Security Program also provides a recommended practices section for control systems on the US-CERT website. Several recommended practices are available for reading or download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[b]

[a] ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, accessed January 17, 2011.

[b] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html

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 Control System Security Program 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.