ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-11-017-01— WELLINTECH KINGVIEW 6.53 REMOTE HEAP OVERFLOW

January 17, 2011

OVERVIEW

Independent security researcher Dillon Beresford reported a heap overflow vulnerability in WellinTech KingView V6.53, which may allow a remote, unauthenticated attacker to execute arbitrary code. ICS-CERT has verified the vulnerability.

WellinTech has developed and released a patch to mitigate this vulnerability, 6.53(2010-12-15). This patch has been validated by both ICS-CERT and the independent security researcher.

AFFECTED PRODUCTS

This vulnerability affects both the Chinese and English language versions of KingView V6.53.

IMPACT

Successful exploitation of the heap overflow vulnerability in KingView V6.53 would allow a remote attacker to cause the service to crash and may allow the execution of arbitrary code as the user.

The specific impact to an individual organization depends on many factors that are unique to the organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on its environment, architecture, and product implementation.

BACKGROUND

According to the WellinTech website, KingView is widely used in power, water, building automation, mining, and other sectors, with most customers in China. It is also used in the Chinese aerospace industry.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

A specially crafted packet sent to port 777/TCP can cause heap corruption when processed by the HistorySrv process. Successful exploitation of this vulnerability can lead a remote unauthenticated attacker to cause a denial of service, or to execute arbitrary code.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

Exploit code is publicly available.

DIFFICULTY

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

MITIGATION

ICS-CERT recommends that users of KingView take the following mitigation steps:

- Implement network or host-based firewall rules to limit network access to Port 777/TCP.
- Upgrade to the latest Version 6.53(2010-12-15) and install the patch. Users can download the patch at:

  http://en.wellintech.com/products/detail.aspx?contentid=25
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.[1]
- Control system networks and devices should be located behind firewalls, and be isolated from the business network. If remote access is required, secure methods such as Virtual Private Networks (VPNs) should be used.

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.*[2]

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

[2] 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.