ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT – 11-011-01 WELLINTECH

January 11, 2011

ALERT

SUMMARY

ICS-CERT has become aware of public reports of a vulnerability in WellinTech KingView v6.53, which could be exploited by remote attackers to take control of a vulnerable system. This issue is caused by a buffer overflow vulnerability in the "HistorySvr.exe" module when processing packets sent to Port 777/TCP. This could be exploited by remote unauthenticated attackers to crash an affected application or execute arbitrary code. Exploit code has been published.

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.

ICS-CERT has not yet verified this vulnerability. ICS-CERT is providing this information as an immediate notification of new activity and is currently working with the CERT Coordination Center (CERT/CC) and US-CERT. Further information will be released as it becomes available.

Please report any issues affecting control systems in critical infrastructure environments to ICS-CERT.

ICS-CERT Operations Center
1-877-776-7585

www.ics-cert.org
ICS-CERT@DHS.GOV

What is an ICS-CERT Alert? An ICS-CERT Alert is intended to provide timely notification to critical infrastructure owners and operators concerning threats or activity with the potential to impact critical infrastructure computing networks.