Alert (ICS-ALERT-11-011-01)

WellinTech KingView Buffer Overflow

Original release date: January 11, 2011 | Last revised: April 25, 2013

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.

Contact Information

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

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
International Callers: (208) 526-0900

For industrial control systems security information and incident reporting: http://ics-cert.us-cert.gov

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/.