ICS-CERT ALERT

ICS-ALERT-12-020-06—WELLINGTECH KINGSCADA INSECURE PASSWORD ENCRYPTION VULNERABILITY

January 20, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report of an insecure password encryption vulnerability with proof-of-concept (PoC) exploit code affecting Wellintech KingSCADA 3.0, a supervisory control and data acquisition/human-machine interface (SCADA/HMI) product. According to this report, the vulnerability is exploitable by decoding the password file. This report was released by Digital Security Research Group without coordination with either the vendor or ICS-CERT.

ICS-CERT has notified WellinTech of this report and has asked the vendor to confirm the vulnerability and identify mitigations. ICS-CERT is issuing this alert to provide preliminary notice of the reported vulnerable products and to begin identifying baseline mitigations that can reduce the risk of cybersecurity attacks exploiting these vulnerabilities.

The report included vulnerability details and PoC exploit code for the following vulnerability:

Vulnerability Type	Exploitability	Impact
Insecure Password Encryption	Local	Ability to log into HMI

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

WellinTech is a software development company specializing in the Automation and Control industry based in Beijing, China. According to WellinTech, they also have branches in United States, Japan, Singapore, Europe, and Taiwan.

According to the WellinTech website, KingSCADA is a Windows-based control, monitoring, and data collection application used across several industries including power, water, building automation, mining, and other sectors.

MITIGATION

ICS-CERT is currently coordinating with WellinTech and the security researcher to identify useful mitigations.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- 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), recognizing that VPN is only as secure as the connected devices.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

The Control Systems Security Program (CSSP) 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]

Organizations that observe any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT CONTACT

ICS-CERT Operations Center
1-877-776-7585
ics-cert@dhs.gov

For CSSP Information and Incident Reporting: www.ics-cert.org

DOCUMENT FAQ

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.

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.

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed January, 20 2012

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed January, 20 2012.