ICS-CERT ADVISORY

ICSA-12-129-01—WELLINTECH KINGSCADA INSECURE PASSWORD ENCRYPTION VULNERABILITY

May 08, 2012

OVERVIEW

This advisory is a follow-up to the alert titled "ICS-ALERT-12-020-06—WellinTech KingSCADA Insecure Password Encryption Vulnerability" that was published January 20, 2012, on the ICS-CERT web page.

Independent researchers Alexandr Polyakov and Alexey Sintsov from DSecRG[a] identified an unsecure password encryption vulnerability in WellinTech KingSCADA application. When KingSCADA OPCServer and OPCClient are not on the same node, a remote attacker may obtain passwords to the system. DSecRG disclosed this vulnerability on its website without coordination with ICS-CERT, the vendor, or any other coordinating entity. An exploit is known to be publicly available.

ICS-CERT has coordinated the mitigation of this vulnerability with WellinTech, which has produced a new version of KingSCADA that resolves the problem. ICS-CERT has not tested this version to verify that the vulnerability is resolved.

AFFECTED PRODUCTS

The following WellinTech KingSCADA versions are affected:

- WellinTech KingSCADA 3.0.

IMPACT

This vulnerability allows an attacker with access to the password storage file to decode all passwords and use those passwords to access the system as a normal user.

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 operational environment, architecture, and product implementation.

a. http://www.dsecrg.com, website last accessed May 08, 2012.

BACKGROUND

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.

The WellinTech website describes KingSCADA as a Windows-based control, monitoring, and data collection application used across several industries including power, water, building automation, mining, and other sectors.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

INSECURE PASSWORD ENCRYPTION[b]

System passwords are stored in a file format that is easy for an attacker to decode. If an attacker is able to access and decode this file, he will be able to log into the system as a normal user or administrator.

CVE-2012-1977[c] has been assigned to this vulnerability. A CVSS V2 base score of 7.2 has also been assigned.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploit(s) are known to target this vulnerability.

DIFFICULTY

An attacker with a low skill level would be able to exploit this vulnerability.

MITIGATION

WellinTech has provided the following link to the latest version of KingSCADA:

http://download.kingview.com/software/KingSCADA/EN/KingSCADA3.1_2012-04-16EN.rar.

According to WellinTech, this new version securely hashes passwords. ICS-CERT has not tested the new version to verify this.

---

b. CWE-311: Missing Encryption of Sensitive Data, http://cwe.mitre.org/data/definitions/311.html, website last accessed May 08, 2012.

c. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1977, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

The Control Systems Security Program (CSSP) also provides a section for control systems security recommended practices on the CSSP web page. Several recommended practices are available for reading and download, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies*.[d] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Organizations observing 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

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 CSSP 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.

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.

d. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed May 08, 2012.