ICS-CERT ALERT

ICS-ALERT-12-212-01—KESSLER-ELLIS PRODUCTS INFILINK HMI INSUFFICIENTLY PROTECTED CREDENTIALS

July 30, 2012

ALERT

SUMMARY

ICS-CERT is aware of a public report of an insufficiently protected credentials vulnerability with proof-of-concept (PoC) exploit code affecting Kessler-Ellis Products (KEP) Infilink HMI V5.00.23, which is a human-machine interface (HMI) product. According to this report, this vulnerability is exploitable locally by using the extracted common password key. ICS-CERT and the vendor were in the initial coordination stages when the report was released on July 29, 2012, at DEFCON 20.

ICS-CERT has notified the affected vendor of the report and has asked the vendor to confirm the vulnerability and identify mitigations. ICS-CERT is issuing this alert to provide early notice of the report and identify baseline mitigations for reducing risks to these and other cybersecurity attacks.

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

Vulnerability Type	Remotely Exploitable	Impact
Insufficiently Encrypted Credentials	No	Unauthorized Access, Access to Sensitive Data

Dr. Wesley McGrew of Mississippi State University disclosed this vulnerability to ICS-CERT prior to presenting the information at the DEFCON 20 conference in Las Vegas, Nevada on July 29, 2012. The KEP Infilink HMI product (V5.00.23) does not securely hash credentials in the project files. The product uses a simple binary XOR against the password to encrypt plaintext credentials. The key is trivial to extract and is common for all installations of the product.

The KEP Infilink HMI software package provides industrial automation that is suited for small Programmable Logic Controller (PLC) users. KEP's products are deployed in multiple sectors.

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

MITIGATION

ICS-CERT is currently coordinating with the vendor and security researcher to identify 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 a 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 Web site. 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
Email: ics-cert@dhs.gov

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

ICS-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

a. ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, Web site last accessed July 30, 2012.

b. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed July 30, 2012.

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.