ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ALERT

ICS-ALERT-12-020-05A—KOYO ECOM100 MULTIPLE VULNERABILITIES

UPDATE A

February 14, 2012

ALERT

SUMMARY

This Alert Update is a follow-up to the original ICS-CERT Alert titled "ICS-ALERT-12-020-05— Koyo Ecom100 multiple vulnerabilities" that was published January 20, 2012, on the ICS-CERT web page.

ICS-CERT is aware of a public report of multiple vulnerabilities with proof-of-concept (PoC) exploit code affecting the Koyo ECOM100 Ethernet Module. This module is used to communicate between a PLC and the control system. This report is based on information presented by Reid Wightman during Digital Bond's SCADA Security Scientific Symposium (S4) on January19, 2012. Vulnerability details were released without coordination with either the vendor or ICS-CERT.

--------- Begin Update A Part 1 of 1 --------

A brute force password cracking tool has been released that targets the weak authentication vulnerability in the ECOM series modules. This tool may greatly reduce the time and skill level required to attack a vulnerable system.

--------- End Update A Part 1 of 1----------

ICS-CERT is attempting to notify the affected vendor of the report to ask the vendor to confirm the vulnerabilities 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 vulnerabilities:

Please see the DHS Disclaimer notice, available here: http://www.us-cert.gov/privacy.html#notify

Vulnerability Type	Exploitability	Impact
Weak Authentication Uses 8-byte passcode	Remote	Loss of Integrity
Replay Attack	Remote	Loss of Integrity
Web Server No Authentication	Remote	Open Authentication / Loss of Integrity
Web Server Buffer Overflow	Remote	Denial of Service
Web Server Cross-Site Scripting (XSS)	Remote	Loss of Integrity
Resource Exhaustion	Remote	Denial of Service and Web Server Crash

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

MITIGATION

ICS-CERT is currently coordinating with Koyo 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.

[a] ICS-CERT ALERT, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, website last accessed February 14, 2012.

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.

[b] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed February 14, 2012.