ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM
CONTROL SYSTEMS SECURITY PROGRAM

ICS-CERT ADVISORY

ICSA-12-102-02—KOYO ECOM MODULES MULTIPLE VULNERABILITIES

April 11, 2012

OVERVIEW

This Advisory is a follow-up to the ICS-CERT Alert titled "ICS-ALERT-12-020-05A— Koyo Ecom100 Multiple Vulnerabilities" that was originally published January 20, 2012, on the ICS-CERT web page and updated on February 14, 2012.

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 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.

A brute force password cracking tool has also 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.

ICS-CERT has coordinated these vulnerabilities with Koyo, which has produced an updated firmware that resolves these vulnerabilities.

AFFECTED PRODUCTS

The following Koyo products and versions are affected:

DIRECTLOGIC DL205 SERIES PROGRAMMABLE LOGIC CONTROLLERS

- H2-ECOM (For DirectLogic DL205 Series Programmable Logic Controllers)
- H2-ECOM-F (For DirectLogic DL205 Series Programmable Logic Controllers)
- H2-ECOM100 (For DirectLogic DL205 Series Programmable Logic Controllers)

DIRECTLOGIC DL06 SERIES PROGRAMMABLE LOGIC CONTROLLERS

- H0-ECOM (For DirectLogic DL06 Series Programmable Logic Controllers)
- H0-ECOM100 (For DirectLogic DL06 Series Programmable Logic Controllers).

This product is provided subject only to the Notification Section as indicated here: http://www.us-cert.gov/privacy/

DIRECTLOGIC DL405 SERIES PROGRAMMABLE LOGIC CONTROLLERS

- H4-ECOM (For DirectLogic DL405 Series Programmable Logic Controllers)
- H4-ECOM-F (For DirectLogic DL405 Series Programmable Logic Controllers)
- H4-ECOM100 (For DirectLogic DL405 Series Programmable Logic Controllers).

IMPACT

Successful exploitation of these vulnerabilities may allow an attacker to load modified firmware, or to perform other malicious activities on the system.

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment, architecture, and product implementation.

BACKGROUND

Koyo is an international manufacturer of automation products and controllers including programmable logic controllers. AutomationDirect.com is a subsidiary of Koyo, and the exclusive distributor of Koyo programmable controllers for North America, South America, Australia, and Europe.

The Koyo ECOM100 Ethernet module is used to communicate between a PLC and the control system.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

BUFFER OVERFLOW[a]

This vulnerability exists because long string input to parameters will cause a buffer overflow, which may allow execution of arbitrary code.

CVE-2012-1805[b] has been assigned to this vulnerability.

MITIGATION

Koyo reports that this is resolved by the patch available for the ECOM modules listed in this Advisory.

[a] http://cwe.mitre.org/data/definitions/119.html, CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer. This website was last accessed April 10, 2012.

[b] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1805, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

WEAK PASSWORD REQUIREMENTS[c]

This vulnerability exists because the ECOM modules only allow use of up to an 8-byte password for authentication. A brute force tool for exploiting this vulnerability has been released publicly.

CVE-2012-1806[d] has been assigned to this vulnerability

MITIGATION

The patch does not change the password length, but it implements a lockout mechanism to mitigate this risk.

WEB SERVER CROSS-SITE SCRIPTING[e]

This vulnerability exists because the web server allows malicious cross-site scripts.

CVE-2012-1807[f] has been assigned to this vulnerability.

MITIGATION

Koyo reports that this is resolved by the patch available for the ECOM modules listed in this Advisory.

WEB SERVER REQUIRES NO AUTHENTICATION[g]

This vulnerability exists because the web server in the ECOM modules does not require authentication to perform critical functions.

CVE-2012-1808[h] has been assigned to this vulnerability.

MITIGATION

According to Koyo, the web server within the ECOM modules are limited to module configuration parameters. Web server authentication was not added to the module; however, the web server is now disabled by default. A configuration change is required to enable the web server.

UNCONTROLLED RESOURCE CONSUMPTION[i]

c. http://cwe.mitre.org/data/definitions/521.html , CWE-521: Weak Password Requirements. This website was last accessed April 10, 2012.

d. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1806, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

e. http://cwe.mitre.org/data/definitions/79.html, CWE-79: Cross Site Scripting. This website was last accessed April 10, 2012.

f. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1807, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

g. http://cwe.mitre.org/data/definitions/306.html , CWE-306: Missing Authentication for Critical Function. This website was last accessed April 10, 2012.

h. http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1808, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

This vulnerability exists because the ECOM web server does not properly restrict the size or amount of resources that are requested or could be influenced by an actor. This can lead to excessive resource consumption, affecting system performance.

CVE-2012-1809[j] has been assigned to this vulnerability.

MITIGATION

According to Koyo, the web server within the ECOM modules is limited to module configuration parameters. Resource management features were not added to the module; however, the web server is now disabled by default. A configuration change is now required to enable the web server.

VULNERABILITY DETAILS

EXPLOITABILITY

These vulnerabilities are all remotely exploitable.

EXISTENCE OF EXPLOIT

Public exploits are known to target these vulnerabilities.

DIFFICULTY

An attacker with a low to moderate skill level would be able to exploit these vulnerabilities.

MITIGATION

According to Automation Direct, the firmware for the ECOM family of Ethernet Products for the Koyo DirectLogic Series of PLCs has been updated to address these vulnerabilities; the update can be downloaded here: http://www.hosteng.com/.

AutomationDirect.com encourages all customers that use and purchase the above products to subscribe to the e-mail firmware notification services for e-mail notification services for future upgrades and updates. Users can subscribe to this notification system at http://notify.automationdirect.com/firmware/.

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.

[i] http://cwe.mitre.org/data/definitions/306.html, CWE-306: Missing Authentication for Critical Function. This website was last accessed April 10, 2012.

[j] http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-1809, NIST uses this advisory to create the CVE website report. This website will be active sometime after publication of this advisory.

- 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.*[k] 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.

[k] CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, website last accessed April 11, 2012.