ICS-CERT ALERT

ICS-ALERT-12-046-01**A**—(UPDATE) INCREASING THREAT TO INDUSTRIAL CONTROL SYSTEMS

October 25, 2012

OVERVIEW

ICS-CERT is monitoring and responding to a combination of threat elements that increase the risk of control systems attacks. These elements include Internet accessible industrial control system (ICS) configurations, vulnerability and exploit tool releases for ICS devices, and increased interest and activity by hacktivist groups and others.

On February 14, 2012, several new exploit tools were publicly released that specifically target programmable logic controllers (PLCs), the building blocks of many ICSs. These exploits target PLCs from GE, Rockwell Automation, Schneider Electric, and Koyo. In addition, one of the exploits targets the EtherNet/IP protocol, which is deployed by numerous PLC vendors in addition to those listed here. The payloads purportedly can affect any device that uses the EtherNet/IP protocol and could allow an attacker to crash or restart affected devices.

--------- Begin Update A Part 1 of 2 --------

A team of researchers recently contacted ICS-CERT with preliminary results from their analytical project to locate Internet facing control system related devices. Using the SHODAN search engine, the researchers compiled a list of more than 500,000 control systems-related devices using supervisory control and data acquisition (SCADA) and other ICS-related search terms. The researchers have brought their findings to the attention of ICS-CERT, citing concerns that an adversary could use the search engine as a shortcut to find vulnerable systems and thereby threaten or attack critical infrastructure. ICS-CERT is working with the researchers and industry partners to notify the owners of the identified IP addresses, but recommends that asset owners and operators take a proactive approach and audit their systems to ensure that strong authentication/logon credentials and defensive measures are in place.

--------- End Update A Part 1 of 2 --------

ICS-CERT is issuing this alert to inform critical infrastructure and key resource (CIKR) asset owners and operators of recent and ongoing activity concerning increased risk to CIKR assets, particularly Internet accessible control systems.

This product is provided subject to the Terms of Use as indicated here: http://www.us-cert.gov/privacy.html#notify

EMERGING THREATS

Multiple threat elements are combining to significantly increase the ICSs threat landscape. Hacktivist groups are evolving and have demonstrated improved malicious skills. They are acquiring and using specialized search engines to identify Internet facing control systems, taking advantage of the growing arsenal of exploitation tools developed specifically for control systems. Asset owners should take these changes in threat landscape seriously, and ICS-CERT strongly encourages taking immediate defensive action to secure their systems using defense-in-depth principles.[a] Asset owners should not assume that their control systems are secure or that they are not operating with an Internet accessible configuration. Instead, asset owners should thoroughly audit their networks for Internet facing devices, weak authentication methods, and component vulnerabilities.

HACKTIVIST GROUP ACTIVITY

ICS-CERT has recently seen a marked increase in interest shown by a variety of malicious groups, including hacktivist[b] and anarchist groups, toward Internet accessible ICS devices. This increased activity includes the identification of Internet facing ICS devices and the public posting of IP address to various Web sites. In addition, individuals from these groups have posted online requests for others to visit or access the identified device addresses.

SPECIALIZED SEARCH ENGINES

The ERIPP[c] and SHODAN search engines can be easily used to find Internet facing ICS devices, thus identifying potential attack targets. These search engines are being actively used to identify and access control systems over the Internet. Combining these tools with easily obtainable exploitation tools, attackers can identify and access control systems with significantly less effort than ever before.

--------- Begin Update A Part 2 of 2 --------

Search engines, such as SHODAN or ERIPP, may be proactively used by owners, operators, and security personnel to audit their networks and devices to locate Internet-facing control system devices that may be susceptible to compromise. Asset owners are encouraged to query various

a. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed October 25, 2012.

b. Hacktivist groups are ideologically motivated hackers who attack entities' networks to promote change or make a political statement. Tactics include Web defacements, redirects, denial of service, information theft, Web site parodies, virtual sit-ins, and virtual sabotage. Some groups are well organized and aim to conduct more malicious attacks to advance their views.

c. Every Routable IP Project, http://eripp.com/, Web site last accessed October 25, 2012.

search engines using the vendor product, model, and version of a device, to determine if their IP address block is found within the search results. If control systems devices are found using these tools, asset owners should take the necessary steps to remove these devices from direct or unsecured Internet access as soon as possible.

--------- End Update A Part 2 of 2 --------

ICS-CERT has released two prior alerts[d,e] warning of the risks associated with Internet accessible devices; the alerts are available on the ICS-CERT Web page.

EXPLOITATION TOOL RELEASES

The increased interest in ICS product security has resulted in a significant increase in product vulnerability reports. Security researchers and others have released tools exploiting vulnerabilities identified in these reports. These targeted exploits are readily available through various software tools and from exploit developers. Easy access to free or low cost exploit tools has dramatically lowered the skill level required for novice hackers and has likewise reduced the development time for advanced attackers.

On February 14, 2012, several independent researchers released exploit tools specifically targeting programmable logic controllers (PLCs), which are the building blocks of many ICSs. These tools include modules that can be plugged into exploit frameworks, such as Metasploit, giving potential attackers another avenue to target ICS. Modules have been released to exploit several major PLC vendors, including:

- GE (D20),
- Schneider Electric (Modicon Quantum),
- Rockwell Automation (Allen Bradley ControlLogix), and
- Koyo (H4-ES).

ICS-CERT is actively coordinating with these vendors and has published specific alerts and advisories to notify ICS stakeholders of this addition to the ICS threat landscape.

MITIGATION

ICS-CERT strongly recommends that asset owners and operators audit device configurations for Internet accessibility, regardless of whether they believe they have Internet accessible devices.

d. ICS-ALERT-11-343-01 – Control System Internet Accessibility, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-343-01.pdf, last accessed October 25, 2012.
e. ICS-ALERT-10-301-01 – Control System Internet Accessibility, http://www.us-cert.gov/control_systems/pdf/ICS-Alert-10-301-01.pdf, last accessed October 25, 2012.

Control systems often have Internet accessible devices installed without the owner's knowledge, putting those systems at increased risk of attack.

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.
- 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.
- Remove, disable, or rename any default system accounts wherever possible.
- Implement account lockout policies to reduce the risk from brute forcing attempts.
- Implement policies requiring the use of strong passwords.
- Monitor the creation of administrator level accounts by third-party vendors.

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

ICS-CERT 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.*[f]

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 industrial control systems security information and incident reporting: www.ics-cert.org

f. Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed October 25, 2012.

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

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.