ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ALERT

ICS-ALERT-11-343-01A—CONTROL SYSTEM INTERNET ACCESSIBILITY

UPDATE A

June 21, 2012

ALERT

SUMMARY

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

This Alert Update is a follow-up to the original ICS-CERT Alert titled ICS-ALERT-11-343-01—Control System Internet Accessibility published to the ICS-CERT Web site on December 09, 2011, and ICS-ALERT-12-027-01—Increasing Risk to Internet Accessible Control Systems published to the ICS-CERT Web site on January 27, 2012.

This update includes additional activity observed by ICS-CERT related to the threat of Internet accessible control systems devices.

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

ICS-CERT is tracking and has responded to multiple reports of researchers using SHODAN[a], Every Routable IP Project[b] (ERIPP), Google, and other search engines to discover Internet facing control systems. ICS-CERT has coordinated this information with the identified control system owners and operators to notify them of their potential vulnerability to cyber intrusion and attack. When appropriate, ICS-CERT also coordinates with the corresponding sector Information Sharing and Analysis Centers (ISACs) or international CERT/CIRT (Computer Incident Response Team) to notify asset owners. In many instances, the exposed systems were unknowingly or unintentionally configured with potentially unsecure access authentication and authorization mechanisms.

[a] SHODAN is a search engine for Internet facing devices. Its database contains devices identified by scanning the Internet for the ports typically associated with HTTP, FTP, SSH, and Telnet. Searches can be filtered by port, hostname, and/or country. Search results include information like HTTP server responses to GET requests, FTP and Telnet service banners and client/server messages exchanged during login attempts, and SSH banners (including server versions). The search engine can be found at: http://www.shodanhq.com, Web site last accessed June 21, 2012.

[b]. ERIPP is a project to connect to every IP address on the Internet. It has a searchable database of IP address that include the DNS Record and Title of each page found.

ICS-CERT works with the asset owner/operators and vendor or systems integrators whenever possible to remove any default credentials and secure these systems from attack. In cases where unauthorized access has been identified, ICS-CERT has assisted control system owners and operators with system and firewall data analysis to determine the extent of the intrusion and whether any configuration changes might have been made to the system.

The use of readily available and generally free search tools significantly reduces time and resources required to identify Internet facing control systems. In turn, hackers can use these tools to easily identify exposed control systems, posing an increased risk of attack. Conversely, owners and operators can also use these same tools to audit their assets for unsecured Internet facing devices.

RECENT REPORTS

Internet facing control systems have been identified in several critical infrastructure sectors. The systems vary in their deployment footprints, ranging from stand-alone workstation applications to larger distributed control systems (DCS) configurations. In many cases, these control systems were designed to allow remote access for system monitoring and management. All too often, remote access has been configured with direct Internet access (no firewall) and/or default or weak user names and passwords. In addition, those default/common account credentials are often readily available in public space documentation. In all cases, ICS-CERT has worked with these organizations to remove default credentials and strengthen their overall security. Recent examples of these are as follows.

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

- ICS-CERT has recently become aware of multiple systems with default usernames and passwords that are accessible via the Internet. These systems have not been configured securely with common best practices such as being placed behind a firewall or changing documented default credentials. These reports include the Echelon i.LON product that is commonly deployed within ICS devices such as motors, pumps, valves, sensors, etc., which contain a default username and password. This is not an inherent vulnerability, but left unchanged, poses a security risk, especially when configured as Internet accessible. The default username and password should be removed and replaced with a strong username and password configuration, especially when the device is Internet accessible.
- ICS-CERT has released several products concerning weak authentication mechanisms. Weak authentication mechanisms are often difficult to remedy because passwords cannot typically be changed by the user to protect the system. The products below highlight weak authentication vulnerabilities that have been reported to ICS-CERT and patched by the vendor:
  - ICSA-11-173-01- ClearSCADA Remote Authentication Bypass

- ICSA-11-356-01- Siemens Simatic HMI Authentication Vulnerability
- ICSA-12-146-01A - RuggedCom Weak Cryptography for Password Vulnerability.

ICS-CERT recommends that organizations audit their control systems and apply patches, and follow vendor-recommended security postures and settings.
--------- End Update A Part 2 of 2 ----------

- In February 2011, independent security researcher Rubėn Santamarta used SHODAN to identify online remote access links to multiple utility companies' supervisory control and data acquisition (SCADA) systems. Mr. Santamarta notified ICS-CERT for coordination with the vendor and the affected control system owners and operators. Further research indicated that many systems were using default user names and passwords.
- In April 2011, ICS-CERT received reports of 75 Internet facing control system devices, mostly in the water sector. ICS-CERT worked with the Water Sector ISAC and the vendor to notify affected control system owners and operators. Many of those control systems had their remote access configured with default logon credentials.
- In September 2011, independent researcher Eireann Leverett contacted ICS-CERT to report several thousand Internet facing devices that he discovered using SHODAN. To date, this response has included international partners and approximately 63 other CERTs in the effort to notify the identified control system owners and operators that their control systems/devices were exposed on the Internet.
- In November 2011, another individual claimed to have directly accessed an Internet facing control system. The report indicated that the individual gained access using default username and password. ICS-CERT notified the affected control system owner and advised the owner to disconnect the control system from the Internet and reconfigure the remote access security. ICS-CERT also coordinated with the SCADA vendor to provide the owner detailed instructions for removing the default logon account.
- Currently, ICS-CERT is coordinating the response to several new reports of Internet facing control systems from independent researchers Billy Rios, Terry McCorkle, Joel Langill, and other trusted sources.

When incidents of this nature are reported, ICS-CERT works with the reporting entity, control system owners and operators, vendors, integrators, ISACs, and other U.S. and international CERT/CIRTs to notify the identified entities and help the mitigate their exposure.

MITIGATION

ICS-CERT recommends that control system owners and operators audit their control systems—whether or not they think their control systems are connected to the Internet—to discover and verify removal of any default administrator level user names and passwords. Because each control system installation is unique, owners and operators may need to contact their system vendor or integrator for assistance with locating and eliminating default accounts.

Owners and operators can also perform a comprehensive control system cybersecurity assessment using the DHS Control Systems Security Program (CSSP) Cyber Security Evaluation Tool (CSET). CSET is a free, downloadable, stand alone software tool that is designed to assist owners and operators to:

1. Determine their current security posture
2. Identify where security improvements can/should be made
3. Map out the existing component/network configuration
4. Output a basic cybersecurity plan.

A CSET fact sheet is available on the CSSP Web page,[c] it explains the self-evaluation process and provides further information and assistance with the tool. The tool can be downloaded online or organizations can contact CSSP to request onsite training and guidance.

In addition, ICS-CERT recommends that control system owners and operators take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, they 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.

[c] http://www.us-cert.gov/control_systems/pdf/CSET4_Assessment_Fact_Sheet.pdf, Web site last accessed June 22, 2012.

The Control System Security Program also provides a recommended practices section for control systems on the US-CERT Web site. Several recommended practices are available for reading or downloading, including *Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.*[d]

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.

ADDITIONAL RESOURCES

ICS-CERT has previously published a Control Systems Analysis Report titled "CSAR—SSH Scanning"[e] that discusses the brute forcing[f] of control system secure shell (SSH) accounts. Many of the tactics, techniques, and procedures (TTPs) used to brute force SSH account usernames and passwords also apply to Web-based human-machine interface (HMI) applications used in control systems.

ICS-CERT has also published an advisory titled ICSA-10-228-01—Vendor Admin Accounts Warning[g] that emphasizes the importance of awareness and control of administrator level accounts installed by vendors.

ICS-CERT CONTACT

ICS-CERT Operations Center
1-877-776-7585
Email: ics-cert@dhs.gov
For Control Systems Security Program (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.

[d] Control System Security Program (CSSP) Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed June 22, 2012.

[e] http://www.us-cert.gov/control_systems/pdf/ICS-CERT%20CSAR-SSH%20SCANNING.pdf, Web site last accessed June 22, 2012.

[f] CAPEC-112: Brute Force, http://capec.mitre.org/data/definitions/112.html, Web site last accessed June 22, 2012.

[g] http://www.us-cert.gov/control_systems/pdf/ICSA-10-228-01.pdf, Web site last accessed June 22, 2012.

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.