ICS-CERT ALERT

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

December 09, 2011

ALERT

SUMMARY

On October 28, 2010, ICS-CERT published an alert titled "ICS-ALERT-10-301-01—Control System Internet Accessibility" on the ICS-CERT web page. The alert warned control system owners and operators that a search engine called SHODAN[a] was being used to locate Internet facing control systems. ICS-CERT is issuing this new alert to warn of an uptick in related activity and urge asset owners and operators to audit their control systems configurations and verify whether or not they are susceptible to an attack via this vector.

ICS-CERT is tracking and has responded to multiple reports of researchers using SHODAN, 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. 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.

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, website last accessed November 29, 2011.

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.

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:

- In February 2011, independent security researcher Ruben 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, website last accessed December 08, 2011.

The Control System Security Program also provides a recommended practices section for control systems on the US-CERT website. 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
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, website last accessed November 29, 2011.
e. http://www.us-cert.gov/control_systems/pdf/ICS-CERT%20CSAR-SSH%20SCANNING.pdf, website last accessed November 29, 2011.
f. CAPEC-112: Brute Force, http://capec.mitre.org/data/definitions/112.html, website last accessed December 02, 2011.
g. http://www.us-cert.gov/control_systems/pdf/ICSA-10-228-01.pdf, website last accessed November 29, 2011.