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

ICS-CERT ALERT

ICS-ALERT-12-034-01—SSH SCANNING ACTIVITY TARGETS CONTROL SYSTEMS

February 03, 2012

OVERVIEW

ICS-CERT is issuing this alert to inform critical infrastructure and key resource (CIKR) asset owners and operators of recent and ongoing activity involving secure shell (SSH)[a] scanning of Internet facing control systems.[b] ICS-CERT is aware that many organizations have been seeing a large number of access attempts by remote attackers. Systems that provide SSH command line access are common targets for "brute force" attacks.

As recently as this week, ICS-CERT received a report from an electric utility experiencing unsuccessful brute force activity against their networks.

WHAT ARE BRUTE FORCE ATTACKS?

A brute force authentication attack attempts to obtain a user's logon credentials by guessing usernames and passwords. Brute force login tools exist for most services that allow remote access. Attackers can use brute force applications, such as password guessing tools and scripts, to automate username and password guessing. Such applications may use default password databases, dictionaries, or rainbow tables that contain commonly used passwords, or they may try all combinations of a character set to guess a password.

To find running SSH services on networks, attackers probe a large number of IPs on Port 22/TCP—the default SSH listening port. If a response from the probe of Port 22/TCP is received, the attacker may initiate a brute force attack.

SCANNING: WHAT TO LOOK FOR

ICS-CERT recommends that organizations monitor network logs for port scans as well as access attempts. Hundreds or thousands of login attempts over a relatively short time period is an indicator of a brute force attack because systems running SSH normally do not receive high volumes of login attempts. However, indication of an attack does not necessarily mean that the organization is the actual intended target. Scans are frequently executed against a wide range of IP addresses looking for any system meeting the attacker's criteria (in this case, systems running SSH).

a. "Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices." http://en.wikipedia.org/wiki/Secure_Shell, website last accessed February 02, 2012.

b. ICS-ALERT-11-343-01—Control System Internet Accessibility, http://www.us-cert.gov/control_systems/pdf/ICS-ALERT-11-343-01.pdf, website last accessed February 03, 2012.

Because high volume scans tend to be quickly discovered, attackers may try to evade intrusion detection systems (IDS) by making only a few careful attempts, then waiting to try again later. Organizations should look carefully for these "quiet" attempts as possible precursors to more direct attacks.

IS SSH RUNNING?

While SSH is popularly associated with UNIX or Linux systems, many types of devices provide SSH access by default, including control systems equipment. Control system devices are often found on networks with SSH enabled by default.

MITIGATION

ICS-CERT strongly encourages CIKR asset owners and operators to examine their control network configurations and establish a baseline configuration and traffic pattern.

ICS-CERT also recommends that asset 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 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.

Control system owners and operators are encouraged to take the following defensive measures to minimize the risk of exploitation of these vulnerabilities.

GENERAL MITIGATIONS

- Minimize network exposure for all control system networks and 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. Stay actively aware of what is on the network by performing periodic port scans (where and when possible).[c]
- 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. Make password lengths long and combine letters, numbers, and special characters. For additional guidance, see Microsoft's Online Privacy and Safety web page: *Create Strong passwords*.[d]

c. ICS-CERT recognizes that control systems environments are often sensitive to port scanning. Organizations should refer to their established internal procedures prior to conducting any cybersecurity-related defensive measures.

- Monitor the creation of administrator level accounts by third-party vendors.

SSH-SPECIFIC MITIGATIONS

- Configure SSH servers to use nonstandard ports. SSH normally listens on Port 22/TCP, but can be configured to listen on any other unused TCP port (the TCP protocol offers 65,535 ports). Because many scanning tools only scan a limited (low) port range by default, selecting a nonstandard high port number can make the SSH less likely to be detected by those tools.
- Restrict access to SSH servers. Only allow access from specific hosts rather than allowing access from anywhere. If the SSH server supports public-key authentication, consider using this as an option to static passwords.
- Use Intrusion Detection/Intrusion Prevention. An intrusion detection system (IDS) monitors networks for malicious activity or policy violations. IDS systems can aid in investigations of system breaches.

  Intrusion prevention systems (IPS) incorporate IDS functionality but also include the ability to block an attack as it is happening, preventing harm to the control system network rather than simply announcing that an attack has occurred.

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

RECOVERY AND REPORTING

Organizations that detect suspicious activity should check their logs to see if any of the attempts were successful. If a successful login attempt from a brute force attack is detected, follow-on steps should be taken to implement a cyber incident response plan.[f] In addition, organizations should carefully adhere to computer forensic best practices to avoid destroying potential evidence.[g]

d. Microsoft Online Privacy and Safety, http://www.microsoft.com/protect/fraud/passwords/create.aspx, website last visited February 03, 2012.
e. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/documents/Defense_in_Depth_Oct09.pdf, website last accessed February 03, 2012.
f. CSSP, Recommended Practice: Developing a Control Systems Cybersecurity Incident Response Capability, http://www.us-cert.gov/control_systems/practices/documents/final-RP_ics_cybersecurity_incident_response_100609.pdf, website last accessed February 03, 2012.
http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html#nogo
g. CSSP, Creating Cyber Forensics Plans for Control Systems, http://www.us-cert.gov/control_systems/practices/documents/Forensics_RP.pdf, website last accessed February 03, 2012.

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 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.