



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT - CONTROL SYSTEMS ANALYSIS REPORT

SSH BRUTE-FORCE SCANNING AND ATTACKS

OVERVIEW

ICS-CERT is aware that many organizations have been seeing a large number of attempts to access industrial control systems by remote attackers. Common targets for these brute-force attacks are systems that provide secure shell (SSH¹) command line access. This activity has been going on for a number of years in the IT sector and demonstrates the need for operators of control systems to understand this threat, what to look for, how to protect network perimeters, and when to report such occurrences.

WHAT ARE BRUTE-FORCE ATTACKS?

A brute-force authentication attack is a method of obtaining a user's authentication credentials by guessing usernames and passwords. Brute-force login tools exist for just about any service that allows remote access. Attackers can use brute-force applications, such as password guessing tools and scripts, to try all the combinations of well-known usernames and passwords. Such applications may use default password databases or dictionaries that contain commonly used passwords, or they may try all combinations of a character set to guess a password.

In order to find running SSH services on networks they are unfamiliar with (or even the entire internet) to brute-force, attackers will probe a large number of IPs on port 22 – the default TCP listening port for SSH. If port 22 responds, a brute force attack may occur.

SCANNING: WHAT TO LOOK FOR

Organizations should check logs for generic port scans as well as system access attempts. If the logs show hundreds or thousands of login attempts over a relatively short time period, the system most likely has been the target of a brute-force attack. This doesn't necessarily mean that the perpetrator is specifically targeting an organization. Instead, scans will often be performed against a wide range of IP addresses looking for any system meeting a certain set of criteria (in this case, systems running SSH).

Due to the wide attack surface of SSH, organizations may see a particularly high number of scans for SSH. These are often easy to spot because unlike web or email traffic, systems running SSH typically only expect infrequent connections from a limited number of IPs.

¹ "**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



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Because these high volume scans can be so visible, some attackers may also try to evade intrusion detection systems by only trying a few careful attempts before waiting to try again later. Organizations should look carefully for these “quiet” attempts, as they may be an indication of a careful, more directed attack.

IS SSH RUNNING?

While SSH is popularly associated with UNIX or Linux workstations and servers, many different and sometimes unexpected types of devices provide SSH access by default, including control systems equipment. Such devices are often on networks with SSH enabled (by default) even if it hasn't explicitly been turned on. Organizations should stay actively aware of what's on their networks by performing periodic port scans² (where and when possible).

SSH IS ENCRYPTED. DOES THAT MAKE IT SECURE?

Despite its wide acceptance, there are still threats and occasionally software vulnerabilities associated with using SSH. For example, common libraries used by many implementations of SSH – like OpenSSL – may be reported. Even so, brute-force password guessing represents a more common threat. Through brute-forcing, passwords may still be guessed by automated tools even without a software vulnerability in SSH or its implementations. The mere fact that an SSH server is running and accessible from the Internet will invite attacks.

MITIGATION

A number of different methods can be used to mitigate this threat. Although any of these options will help, it is best to practice defense in depth by protecting systems using multiple defensive techniques. Here are several methods to consider:

- 1. Hide systems running services such as SSH behind a firewall**

Connecting control systems components to the Internet is a significant risk. If a control system component does require Internet connectivity, such devices should be carefully deployed, and appropriate security measures should be implemented. Firewalls provide the capability to hide internal systems and define rules for communication with devices and between different network segments. Of critical importance to control systems is how the firewall is implemented. Many types of firewalls are available, and some research is required to ascertain what type of firewall is right for a given control architecture. Also, consider the use of virtual private networks (VPNs) to access services from outside the control system network, rather than opening up access through a firewall.

- 2. Use strong passwords or public-key authentication**

² ICS-CERT recognizes that port scans are not always viable in control systems environments. Organizations should refer to their established internal procedures prior to conducting any defensive measures.



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Make password lengths long and combine letters, numbers, and special characters. For additional guidance, see Microsoft's "Strong passwords: How to create and use them."³ If the SSH server supports public-key authentication, consider using this as an option to static passwords.

3. Configure SSH servers to use a non-standard port

SSH normally listens on TCP Port 22, but can be configured to listen on any other unused port. The TCP protocol provides 65,535 ports from which to select. The popular port scanning tool Nmap⁴ only scans a little over 1,600 ports by default, so by selecting a nonstandard high port number, SSH may not be detected by scans looking specifically for it.

4. Restrict access to SSH servers

Only allow access from specific hosts rather than allowing access from anywhere.

5. Utilize Intrusion Detection/Intrusion Prevention

An intrusion detection system (IDS) is a device or application that monitors networks or systems for malicious activity or policy violations. IDS systems are the last line of defense and can aid in investigations of system breaches.

Intrusion prevention systems (IPS) incorporate all IDS functionality and then take intrusion detection a step further with the ability to block an attack as it is happening; thereby preventing harm to the network or control system, rather than simply generating an alert when the attack occurs.

For more information on these mitigations strategies and how to create a defense-in-depth security program for control system environments, visit CSSP [Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defense-In-Depth Strategies](#).

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 plan⁵. In addition, organizations should carefully adhere to computer forensic best practices to avoid destroying potential evidence⁶.

³ Microsoft Online Safety, <http://www.microsoft.com/protect/fraud/passwords/create.aspx>, website last visited February 18, 2010.

⁴ Nmap Website, <http://nmap.org/>, website last visited February 18, 2010.

⁵ See DHS Control Systems Security Program's paper on Incident Response for further information: http://csrp.inl.gov/Documents/final-RP_ics_cybersecurity_incident_response_100609.pdf

⁶ http://www.us-cert.gov/control_systems/pdf/Forensics_RP.pdf



ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Organizations should follow their established internal procedures if any suspected malicious activity is observed, and report their findings to ICS-CERT for correlation against other incidents. ICS-CERT reminds organizations that proper impact analysis and risk assessment should be performed prior to taking defensive measures.

CONTACT ICS-CERT:

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@dhs.gov

Toll Free: 1-877-776-7585

For Incident Reporting and Situational Awareness:

www.ics-cert.org

For general Control System Security Program Information

http://www.us-cert.gov/control_systems/