ICS-CERT ALERT

ICS-ALERT-10-301-01 – CONTROL SYSTEM INTERNET ACCESSIBILITY
October 28, 2010

SUMMARY

The ICS-CERT has recently received several reports from multiple independent security researchers who have employed the SHODAN search engine[1] to discover Internet facing SCADA systems using potentially insecure mechanisms for authentication and authorization. The identified systems span several critical infrastructure sectors and vary in their deployment footprints. ICS-CERT is working with asset owners/operators, Information Sharing and Analysis Centers (ISACS), vendors, and integrators to notify users of those systems about their specific issues; however, due to an increase in reporting of these types of incidents, ICS-CERT is producing a more general alert regarding these issues.

In most cases, the affected control system interfaces were designed to provide remote access for monitoring system status and/or certain asset management features (i.e., configuration adjustments). The identified systems range from stand-alone workstation applications to larger wide area network (WAN) configurations connecting remote facilities to central monitoring systems. These systems have been found to be readily accessible from the Internet and with tools, such as SHODAN, the resources required to identify them has been greatly reduced.

In addition to the increased risk of account brute forcing[2] from having these systems available on the Internet, some of the identify systems continue to use default user names and passwords and/or common vendor accounts[3] for remote access into these systems. These default/common accounts can in many cases be easily found in online documentation and/or online default password repositories. Control System owners and operators are advised to audit their control systems —whether or not directly connected to the Internet— for the use of default administrator level user names and passwords.

ADDITIONAL MATERIAL

ICS-CERT has previously published Control Systems Analysis Report "CSAR - SSH Scanning"[2] that discusses the brute forcing of control system secure shell (SSH) accounts. Many of the tactics, techniques, and procedures that can be used to brute force SSH account usernames and passwords, also applies to web-based human-machine interface (HMI) systems.

The ICS-CERT has also published an Advisory "ICSA-10-228-01 — Vendor Admin Accounts Warning,"[3] that discusses the importance of owner/operator awareness and control of administrator level accounts

[1] 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). Search engine can be found at: http://www.shodanhq.com.

[2] http://www.us-cert.gov/control_systems/pdf/ICS-CERT%20CSAR-SSH%20SCANNING.pdf.

[3] http://www.us-cert.gov/control_systems/pdf/ICSA-10-228-01%20Non-Authorized%20Admin%20Accounts.pdf.

installed on control systems by third-party vendors. This Advisory is available on the ICS-CERT public web site.[3]

RECOMMENDATIONS

ICS-CERT recommends:

- Placing all control systems assets behind firewalls, separated from the business network
- Deploying secure remote access methods such as Virtual Private Networks (VPNs) for remote access
- Removing, disabling, or renaming any default system accounts (where possible)
- Implementing account lockout policies to reduce the risk from brute forcing attempts
- Implementing policies requiring the use of strong passwords[4]
- Monitoring the creation of administrator level accounts by third-party vendors.[3]

ICS-CERT CONTACT INFORMATION

Please report any issues affecting control systems in critical infrastructure environments to the ICS-CERT.

ICS-CERT Operations Center
1-877-776-7585
www.ics-cert.org
ICS-CERT@DHS.GOV

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.

[4] http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf.