Harden Network Devices

June 2016

Hardening network devices reduces the risk of unauthorized access into the network infrastructure. Vulnerabilities in device management and configurations present weaknesses for the adversary to exploit and maintain persistence within the network.

Adversaries are shifting their focus from the exploitation of hosts to routers and switches. This is done through manipulating weaknesses in the configuration, controlling routing protocols and implanting malware in the operating systems.

Service Security Recommendations

All networking devices, including routers and switches, come equipped with services turned on when received from the manufacturer. Disabled services cannot be exploited by the adversary, therefore, all unnecessary services should be disabled. By default, each manufacturer turns off different services in their standard out-of-the-box configuration, and default services may vary between operating systems. Research should be done to determine what services are running by default. The following guidance will serve to determine the services that should be enabled or disabled:

Enable

- **SSHv3 or TLS:** Both of these protocols are used to securely communicate to remote network devices

Disable

- **Echo Protocol:** A legacy protocol to measure round trip time of a packet
- **Chargen Protocol:** A legacy protocol that uses arbitrary characters to test, debug, and measure the connection
- **Discard Protocol:** A legacy protocol to simply discard received packets
- **Daytime Protocols:** Returns ASCII character strings of current date and time
- **FTP Protocol:** Allows users to copy files between their local system and any system that can be reached on the network
- **Telnet:** An application layer clear text protocol used on the network to communicate with another device
- **BootP service:** A legacy protocol used to assign an IP Address to a device
- **HTTP server:** Most devices come with a Web service enabled by default
- **SNMP protocol:** A protocol to manage network devices. If needed, only run SNMP v3 and do not use SNMP community strings
- **Discovery Protocols:** These protocols are used to share information with neighboring devices and discover the platform of those devices
- **IP source routing:** Allows the sender to control the route of information to the destination
- **IP Unreachable:** ICMP protocol can be used to map out the network topology
- **IP Mask Reply:** Replies respond to ICMP mask requests by sending out ICMP mask replies containing important network information

Interface and Switch Port Recommendations

As with services, all router interfaces and switch ports that are not used should be disabled to prevent unauthorized access to the device.

- Enable port security
- Shutdown unused interfaces
- Place unused switch ports in a VLAN that is not routed and closely monitored. Reassign the native VLAN

Disable

- Unused interfaces and routing protocols
- IP direct-broadcast
- IP proxy-arp

Harden Network Devices

Secure Access Recommendations

There are several ways to access network devices: through an administration connection, console line, auxiliary line, and virtual terminal connection. Each method to access network devices should be secured to prevent any unauthorized access to the network device. The following security configurations need to be implemented to limit and secure access to the router or switch from the console, auxiliary, and VTY ports:

- Use multi-factor authentication using hardware tokens and passwords.
- Use out-of-band management.
- Implement the manufacturer's configuration guidance to restrict access to the console port.
- Limit the number of connections.
- Implement a minimum password length of 14 characters including uppercase, lowercase, numbers, and symbols.
- Use the strongest password encryption available.
- Reduce the risk of exposing administrative interfaces to user traffic by applying IP address access control lists.
- Restrict physical access to routers/switches and apply access control lists for remote access.
- Monitor and log all attempts to access network devices.

Vendors of network infrastructure devices often provide detailed documentation with security guidance for each product. In addition to applying the above mitigations, it is also recommended to apply the security guidelines available through vendor publications.

General Security Recommendations

- Create and enforce the Site Security Policy (SSP) to secure all devices. The SSP should outline roles and responsibilities to manage and monitor devices and services. Each role should only have the lowest privilege access that is required to perform required tasks.
- Backup configuration files and store offline.
- Never share configuration files by using unsecure means, such as email, FTP, or publishing to a website. This could allow the adversary to gain insight into the enterprise architecture or decrypt password hashes.
- Implement multi-factor authentication using hard tokens to securely access routers and switches.
- Use an Out-of-Band management solution to separate network administration traffic from normal user traffic.
- Disable unused services and implement an access control list to protect services that are required by the SSP.
- All updated patches should be tested before implementing on the enterprise to ensure operational network stability and legacy application work.
- Install the latest version of the network device operating system and approved patches to protect from known vulnerabilities to the vendor's equipment.
- Periodically test the security of the network devices and compare the configuration against the site SSP or original configuration to verify the configuration of all network equipment.
- Compare offline hash of the operating system against the hash of the vendor's known good operating system image to validate the integrity.
- Safeguard configuration files with encryption and/or password protection when sending them electronically and when they are stored and backed up.

Contact Information

Industry Inquiries:
Business Affairs Office
410-854-6091
email: bao@nsa.gov

Client Requirements and General Information Assurance Inquiries:
IAD Client Contact Center
410-854-4200
email: IAD_CCC@nsa.gov

Disclaimer: The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.