Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
PART OF THE GCSB

Enhanced Visibility and Hardening Guidance for Communications Infrastructure

Publication: December 3, 2024

U.S. Cybersecurity and Infrastructure Security Agency
U.S. National Security Agency
U.S. Federal Bureau of Investigation
Australian Signals Directorate's Australian Cyber Security Centre
Canadian Centre for Cyber Security
New Zealand's National Cyber Security Centre

Introduction

The Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), Federal Bureau of Investigation (FBI), Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC), Canadian Centre for Cyber Security (CCCS), and New Zealand's National Cyber Security Centre (NCSC-NZ) warn that People's Republic of China (PRC)-affiliated threat actors compromised networks of major global telecommunications providers to conduct a broad and significant cyber espionage campaign. The authoring agencies are releasing this guide to highlight this threat and provide network engineers and defenders of communications infrastructure with best practices to strengthen their visibility and harden their network devices against successful exploitation carried out by PRC-affiliated and other malicious cyber actors. Although tailored to network defenders and engineers of communications infrastructure, this guide may also apply to organizations with on-premises enterprise equipment. The authoring agencies encourage telecommunications and other critical infrastructure organizations to apply the best practices in this guide.

As of this release date, identified exploitations or compromises associated with these threat actors' activity align with existing weaknesses associated with victim infrastructure; no novel activity has been observed. Patching vulnerable devices and services, as well as generally securing environments, will reduce opportunities for intrusion and mitigate the actors' activity.

Strengthening Visibility

In the context of this guide, visibility refers to organizations' abilities to monitor, detect, and understand activity within their networks. High visibility means having detailed insight into network traffic, user activity, and data flow, allowing network defenders to quickly identify threats, anomalous behavior, and vulnerabilities. Visibility is critical for network engineers and defenders, particularly when identifying and responding to incidents.

Monitoring

Network Engineers

- Closely scrutinize and investigate any configuration modifications or alterations to network devices such as switches, routers, and firewalls outside of the change management process. Implement comprehensive alerting mechanisms to detect unauthorized changes to the network, including unusual route updates, enabled weak protocols, and configuration changes (i.e., changes to users and Access Control Lists [ACLs]).
  - Store configurations centrally and push to devices. Do not allow devices to be the trusted source of truth for their configuration. Monitor configuration and, if feasible, test and override on a frequent basis.
- Implement a strong network flow monitoring solution. This solution should allow for network flow data exporters and the associated collectors to be strategically centered around key ingress and egress locations that provide visibility into inter-customer traffic.

- If feasible, limit exposure of management traffic to the Internet. Only allow management via a limited and enforced network path, ideally only directly from dedicated administrative workstations.
- Monitor user and service account logins for anomalies that could indicate potential malicious activity. Validate all accounts and disable inactive accounts to reduce the attack surface. Monitor logins occurring internally and externally from the management environment.
- Implement secure, centralized logging with the ability to analyze and correlate large amounts of data from different sources. Encrypt any logging traffic destined for a remote destination via IPsec, TLS, or any other available encrypted transport options. Additionally, store copies of logs off-site to ensure they cannot be modified or deleted. Enable logging and auditing on devices and ensure logs can be offloaded from the device.
  - If possible, implement a Security Information and Event Management (SIEM) tool to analyze and correlate logs and alerts from the routers for rapid identification of security incidents.
  - Ensure logging takes place at all levels of the environment, network operating system, application, and software levels, as it pertains to network devices.
  - Establish a baseline of normal network behavior and define rules on security appliances to alert on abnormal behavior.
- Ensure the inventory of devices and firmware in the environment are up to date to enable effective visibility and monitoring.

Network Defenders

- Implement a monitoring and network management capability that, at a minimum, enforces configuration management, automates routine administrative functions, and alerts on changes detected within the environment, such as connections and user and account activity.
  - Establish understanding of the architecture of infrastructure and production enclaves, as well as where the two environments meet or are segregated. Map and understand boundary and ingress/egress points of the network management enclave.
  - Understand which assets should be forward facing and remove those that should not be forward facing. Closely monitor all devices that accept external connections from outside the corporate network and investigate any configurations that do not comply with known good configurations, such as open ports, services, or unexpected Generic Routing Encapsulation (GRE) or IPsec tunnel usage. Threat actors have been observed taking advantage of external-facing vulnerable services and features; therefore, proper visibility of network and security operations is vital.
  - If appropriate, implement a packet capture capability as part of the broader visibility effort for the enterprise. Determine capture location(s) and retention policies based on organizational demands.

Hardening Systems and Devices

Hardening device and network architecture is a defense-in-depth strategy. Reducing vulnerabilities, improving secure configuration habits, and following best practices limit potential entry points for PRC-affiliated and other cyber threats.

Protocols and Management Processes

Network Engineers

- Use an out-of-band management network that is physically separate from the operational data flow network. Ensure that management of network infrastructure devices can only come from the out-of-band management network. In addition, confirm that the out-of-band management network does not allow lateral management connections between devices to prevent lateral movement in the case that one device becomes compromised. Ensure device management is physically isolated from the customer and production networks. When properly implemented, out-of-band management can mitigate many threat actor tactics, techniques, and procedures (TTPs).
- Implement a strict, default-deny ACL strategy to control inbound and egressing traffic. Ensure all denied traffic is logged. For maximum depth, implement on separate devices from those implementing other security controls.
- Employ strong network segmentation via the use of router ACLs, stateful packet inspection, firewall capabilities, and demilitarized zone (DMZ) constructs. Separation via virtual local area networks (VLANs) and, if possible, private VLANs (PVLAN) will provide additional granular logical separation. This should be done as part of a broader defense-in-depth approach that protects and isolates different device groups.
  - Place externally facing services, such as Domain Name System (DNS), web servers, and mail servers, in a DMZ to provide segmentation from the internal LAN and backend resources.
  - Additionally, as a general strategy, put devices with similar purposes in the same VLAN. For example, place all user workstations from a certain team in one VLAN, while putting another team with different functions in a separate VLAN.
  - Do not manage devices from the internet. Only allow device management from trusted devices on trusted networks. Use dedicated administrative workstations (DAWs) connected to dedicated management zones.
- Harden and secure virtual private network (VPN) gateways by limiting external exposure, if possible, and limiting the port exposure to what is minimally required (for example udp/500, udp/4500 and protocol type 50 (ESP)). Ensure all VPNs are configured to only use strong cryptography for key exchange, authentication, and encryption.[1]
  - Disable unused VPN features and cryptographic algorithms to prevent exploitable weaknesses.
- Ensure that traffic is end-to-end encrypted to the maximum extent possible.

- As a management policy, control access to device Virtual Teletype (VTY) lines with an ACL to restrict inbound lateral movement connections.
  - Additionally, disable outbound connections to mitigate against lateral movement. Monitor for changes as adversaries can modify this configuration on compromised devices to allow outbound connections.
- Ensure all authentication, authorization, and accounting (AAA) logging is securely sent to a centralized logging server with modern confidentiality, integrity, and authentication (CIA) protections.
- If using Simple Network Management Protocol (SNMP), ensure only SNMP v3 with encryption and authentication is used, along with ACL protections against unnecessary public exposure. Ensure configuration with the most secure cryptographic options supported by the hardware.
- Disable all unnecessary discovery protocols, such as Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP). If they are required, only enable on the necessary interfaces.
- Ensure Transport Layer Security (TLS) v1.3 is used on any TLS-capable protocols to secure data in transit over a network.[2] Ensure TLS is configured to only use strong cryptographic cipher suites.[3]
  - Use Public Key Infrastructure (PKI)-based certificates instead of self-signed certificates.
  - Implement a robust process to renew certificates before they expire.
- Disable Internet Protocol (IP) source routing.
- Disable Secure Shell (SSH) version 1. Ensure only SSH version 2.0 is used with the following cryptographic considerations.[2] For more information on acceptable algorithms, see NSA's Network Infrastructure Security Guide.
  - Configure with minimally a 3072-bit RSA key.
  - Configure with minimally a 4096 Diffie-Hellman key size (group 16).
- When possible, apply secure authentication to protocols and services which allow it, such as Network Time Protocol (NTP), Terminal Access Controller Access-Control System (TACACS+), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Hot Standby Router Protocol (HSRP). Similarly, disable any unauthenticated management protocols or functions, such as Cisco Smart Install.
- Use secure cryptographic building blocks when building VPNs such as [3]:
  - Key Exchange:
    - Diffie-Hellman Group 15 with 3072-bit Modular Exponential (MODP)
    - Diffie-Hellman Group 16 with 4096-bit Modular Exponential (MODP)
    - Diffie-Hellman Group 20 with 384-bit Elliptic Curve Group (ECP)
  - Encryption: AES-256
  - Hashing: SHA-384 or SHA-512
- Ensure that no default passwords are used.
  - Change all default passwords on first use.

  - Ensure no passwords are reset back to the default.
- Confirm the integrity of the software image in use by using a trusted hashing calculation utility, if available.
  - If a utility is unavailable, calculate a hash of the software image on a trusted administration workstation and compare against the vendor's published hashes on an authenticated site as a trusted source of truth. This may require engaging the device's maintenance contract to access source of truth hash values. For additional security, copy the image to a forensic workstation and calculate the hash value to compare against the vendor's published hashes.

Network Defenders

- Disable any unnecessary, unused, exploitable, or plaintext services and protocols, such as Telnet, File Transfer Protocol (FTP), Trivial FTP (TFTP), SSH v1, Hypertext Transfer Protocol (HTTP) servers, and SNMP v1/v2c. Ensure any required internet-exposed services are adequately protected by ACLs and are fully patched.
- Conduct port-scanning and scanning of known internet-facing infrastructure to ensure no additional services are accessible across the network or from the internet. Remove unnecessary internet-facing infrastructure, monitor necessary internet-facing infrastructure, and continuously validate the architecture.
  - Routers with an active shell environment—even if they have not been tampered with—have significantly more listeners running at the operating system (OS) level compared to the software level.

Network defenders and network engineers should ensure close collaboration and open communication to accomplish the following:

- Ensure all networking configurations are stored, tracked, and regularly audited for compliance with security policies and best practices.
  - Whenever networking configurations are transmitted for storage, tracking, and troubleshooting, confirm that they are sent using encrypted protocols. Additionally, be sure they are not attached to plaintext emails or sent via FTP or TFTP.
- Monitor for vendor end-of-life (EOL) announcements for hardware devices, operating system versions, and software, and upgrade as soon as possible.
- Implement a change management system that anticipates both routine and emergency patching. Continuously monitor for vendor vulnerability and patch announcements and ensure patches are applied in a timely manner. Ensure use of vendor recommended version of the operating system for the features and capabilities required.
  - Test and validate patches as part of the change and patch management processes.
- As part of a broader password policy, store passwords with secure hashing algorithms. Passwords should meet complexity requirements and should be stored using one-way hashing algorithms or, if available, unique keys. Follow National Institute of Standards and Technologies guidelines when creating password policies.

- Require phishing-resistant multi-factor authentication (MFA) for all accounts that access company systems, networks, and applications, including sensitive administrative access to routers. MFA should use a combination of credentials and a phishing-resistant secondary verification method, such as hardware-based PKI or FIDO authentication, to ensure secure access and prevent unauthorized entry.
- As part of a broader identity and access management policy, use local accounts only for emergencies and change the passwords after each use. Verify that each use was authorized and expected. For everyday management of network infrastructure, use a centralized AAA server that supports multi-factor authentication requirements; however, ensure the AAA server is not linked to the primary corporate identity store.
- Limit session token durations and require users to reauthenticate when the session expires. Conduct audits to determine the standard session duration for each role to implement session expirations.
- Implement a Role-Based Access Control (RBAC) strategy that assigns users to a specific role with defined and inherited permissions to better control and manage what users can do.
- Remove any unnecessary accounts and periodically review accounts to verify that they continue to be needed. Apply the principle of least privilege to make sure accounts only have the minimum permissions necessary to complete their tasks. Additionally, continuously monitor accounts in use.

Cisco-Specific Guidance

Organizations in the communications sector should be aware that the authoring agencies have observed Cisco-specific features often being targeted by, and associated with, these PRC cyber threat actors' activity. To address the risk of exploitation by these specific threat actors, the authoring agencies urge organizations to apply the following hardening best practices to all Cisco operating systems. For additional information, see Cisco's IOS XE Hardening Guide and Guide to Securing NX-OS Software Devices.

- Disable Cisco's Smart Install service using `no vstack`.
- If not required, disable the guestshell access using `guestshell disable` for those versions which support the guestshell service.
- Disable all non-encrypted web management capabilities. If web management is required, configure servers in compliance with vendor recommended security settings and software images.
  - Always disable the underlying non-encrypted web server using `no ip http server`. If web management is not required, disable all of the underlying web servers using `no ip http server` and `no ip http secure-server`.
- Disable telnet and ensure it is not available on any of the VTY lines by configuring all VTY stanzas with `transport input ssh and transport output none`.
- To securely store passwords on Cisco devices, organizations should:
  - Use Type-8 passwords when possible.

- Avoid use of deprecated hashing or password types when storing passwords, such as Type-5 or Type-7.
- If supported, secure the TACACS+ key as a Type-6 encrypted password.

Incident Reporting

- **U.S. organizations:** If suspicious activity is identified, contact your local FBI field office or the FBI's Internet Crime Complaint Center (IC3). Cyber incidents can also be reported to CISA by calling 1-844-Say-CISA (1-844-729-2472), emailing report@cisa.dhs.gov, or reporting online at cisa.gov/report. For NSA client requirements or general cybersecurity inquiries, contact Cybersecurity_Requests@nsa.gov.
- **Australian organizations:** Visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and access alerts and advisories.
- **Canadian organizations:** Report incidents by emailing CCCS at contact@cyber.gc.ca.
- **New Zealand organizations:** Report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

Secure by Design

The authoring agencies urge software manufacturers to incorporate secure by design principles into their software development lifecycle to strengthen the security posture of their customers. Software manufacturers should prioritize secure by design configurations to eliminate the need for customer implementation of hardening guidelines. Additionally, customers should demand that the software they purchase is secure by design. For more information on secure by design, see CISA's Secure by Design webpage. Customers should refer to CISA's Secure by Demand guidance for additional product security considerations.

Resources

- CISA: Cross-Sector Cybersecurity Performance Goals
- Joint Guide: Best Practices for Event Logging and Threat Detection
- NSA: Network Infrastructure Security Guide
- NSA, CISA, and FBI: People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices
- NSA: Hardening Network Devices
- NSA: Performing Out-of-Band Network Management
- NSA: Cisco Password Types: Best Practices
- NSA: Cisco Smart Install Protocol Misuse
- CCCS: Cryptographic Algorithms for UNCLASSIFIED, PROTECED A, and PROTECTED B Information – ITSP.40.111

- NIST: Special Publication 800-52: Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations
- NIST: Special Publication 800-77: Guide to IPsec VPNs

References

[1] CCCS: Guidance on Securely Configuring Network Protocols

[2] NSA: Network Infrastructure Security Guide

[3] CNSS: Committee on National Security Systems Policy (CNSSP)-15

Disclaimer

The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies. Additionally, the information in this document is provided "as-is" and without warranties or representations of any kind. The users of this information shall have no recourse against the authoring parties for any loss, liability, damage or cost that may be suffered or incurred at any time arising from the use of information in this document, including but not limited to loss of data or interruption of business.

Acknowledgements

Cisco and Google Cloud Security contributed to this guidance.

Version History

December 3, 2024: Initial version.