CYBER SECURITY ADVISORY

April 15, 2025

Authored by:

People's Republic of China Targeting Network Edge Routers: Observations and Mitigation Strategies

ISBN 978-0-660-76965-3
CAT D96-128/2025E-PDF

Communications Security Establishment Canada
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications Canada
Centre canadien pour la cybersécurité

Canada

Foreword

This cyber security advisory is intended for IT professionals and managers within government and all sectors.

Effective Date

This publication takes effect on April 15, 2025

Revision History

Revision	Amendments	Date
1	First release.	April 15, 2025

1 Background

A Cyber security advisory is used to raise awareness of a recently identified cyber threat that may impact cyber information assets, and to provide additional mitigation advice to recipients. The Canadian Centre for Cyber Security (Cyber Centre) is able to provide additional assistance regarding the content of this bulletin to recipients as requested.

The Cyber Centre has observed increasing levels of the People's Republic of China threat actor activity, including activity associated to SALT TYPHOON, targeting network edge routers across critical infrastructure sectors. The Cyber Centre and our partners have recently observed repeated compromises of misconfigured and unpatched routing devices.

The Cyber Centre is urging the Canadian cybersecurity community to bolster their awareness of threat actor activity targeting network edge routers and to leverage Cyber Centre guidance to protect their networks.

2 Security and Edge Devices

As we note in the National Cyber Threat Assessment 2025-2026 [10], threat actors are exploiting vulnerabilities in security and network edge routing devices that sit at the perimeter of networks. The Cyber Centre is particularly highlighting that by compromising network edge routers, a threat actor can enter a network, monitor, modify, and exfiltrate network traffic flowing through the device, or possibly move deeper into the victim network.

Given their outward facing presence on the Internet, edge routers are easily identifiable by threat actors. Threat actors often compromise network perimeter defenses by exploiting known vulnerabilities in edge devices. These security weaknesses are usually already identified, and patches are available to fix them. However, breaches occur because these patches are not consistently applied or implemented in a timely manner. We strongly recommend following our guidance in the Government of Canada's Patch Management Guidance publication [3]. In particular, all guidance, manuals and references provided with edge device equipment should be reviewed to ensure organizations adherence to the manufacturer's security guidance. If that guidance is not clear or available, then organizations should reach out to their vendors as needed for support.

The Cyber Centre's Security considerations for Edge Devices [2] also provides the following factors your organization should consider when evaluating the security of an edge device:

- how it is made (the responsibility of the manufacturer)
- how it is configured (a shared responsibility between the manufacturer, through vendor hardening guides and through the organization)
- when the most recent software, firmware, operating system, and security updates and patches were applied

3 Known avenues of exploitation and persistence

The following are examples of known patterns in threat actors' exploitation of edge routers.

3.1 Exposed Services to the Internet

Devices exposing services of any kind to the Internet will easily and rapidly be detected by adversarial actors through mass scanning campaigns and more targeted reconnaissance activity. Sensitive or administrative services such as management protocols are of particular interest to adversaries seeking to identify and exploit edge routers.

3.2 Poor configuration on Device

The Cyber Centre has observed weak cryptography or default security settings configured and not updated that has led to exploitation of those devices. It is important to review manufacturer guidance for hardening edge routers, and to continually review and audit for compliance. Default setting(s) may also include insecure ports or protocols listening on untrusted interfaces. Even though a device is installed and configured properly at the beginning of its lifecycle, as time goes on those configurations can become less secure due to external factors. If a router is compromised, inadequate network segmentation and the absence of Access Control Lists can enable an adversary to more easily move laterally within the network.

3.3 Modifying Configuration Files

Trusted partners have observed that compromised edge routers often have their configurations altered to enable persistent mechanisms and techniques for lateral movement. This includes the establishment of traffic captures, the creation of new administrative accounts, and the configuration of traffic forwarding. Any configurable allow lists should also be reviewed to ensure that no unauthorized additions have been made. Typically, these modifications are executed using the devices' inherent functions and capabilities.

3.4 Exfiltrating Configuration Files

Trusted partners have observed that compromised edge routing devices within Canada have had their configuration files exfiltrated out of their networks by threat actors. By exfiltrating configuration files, threat actors can extract additional sensitive information, perform tests, or identify further vulnerabilities to enable their access. Where configuration files contain credentials and especially those who are not cryptographically secure, threat actors can also use tactics such as offline password cracking to gain further access. Trusted partner reporting indicates that many of the exfiltrated configuration files contained deprecated hashing and password types, such as Type-4 and Type-7 [9].

3.5 Unauthorized Commands

Once an edge router has been compromised, threat actors run unauthorized commands to deepen their access or persistence on the host or network. Identifying suspicious or malicious use of successful unauthorized commands can often be a strong starting point for threat hunts and forensic investigations. Some common threat actor tactics include:

- clearing logs and other records
- adding new threat actor-controlled accounts to the device
- brute forcing and abnormal logins
- making unapproved changes to configuration files

The Cyber Centre has observed threat actors modifying the configurations of edge routers. It is important to conduct regular reviews of these configurations to detect any unauthorized changes. Look out for signs of tampering, such as unrecognized IP addresses and newly added accounts, as well as any unusual packet capture settings that may have been introduced.

3.6 Weak Credentials

The Cyber Centre has observed many cases where devices were compromised due to the use of default or easily guessable passwords.

- Do not use easily guessed passwords, passphrases, or PINs, such as "password", "let me in", or "1234". Even if the passwords or passphrases include character substitutions like "p@ssword"
- Do not use common expressions, song titles or lyrics, movie titles, or quotes
- Do not use your personal details such as your birthday, hometown, or pet's name
- Do not use the passwords assigned by the vendor when installing or enabling new hardware or software
- Do not use passwords found on known data breaches
- Do not reuse password across devices or deployments

4 Remediations

The Cyber Centre has published guidance for organizations and has guidance for enhancing the security posture of edge devices [1][4][5][6][7][8].

In addition to reviewing and implementing that guidance above, the Cyber Centre recommends the following remediations:

- disable unnecessary services especially unsecured services such as Telnet, HTTP and SNMP versions (v1/v2c)
- disable any unauthenticated router management protocols or functions
- ensure that SNMP v3 is configured with encryption and authentication
- restrict device management to administrators inside secured management networks, avoiding direct internet access to management interfaces
- use phishing-resistant MFA for all administrative access, preferably using hardware-based PKI or FIDO authentication
- use secure modern encryption standards, such as AES-256 and ensure TLS v1.3 is utilized with strong cipher suites for secure communications
- use strong, non default passwords
- apply secure authentication to protocols and services which support it
- upgrade deprecated hashing mechanisms and password types
- ensure that devices are running vendor-recommended firmware versions
- validate software integrity of images using hash verification against authenticated vendor hashes
- implement secure, centralized logging with capabilities to analyze large datasets
- encrypt logging traffic to avoid tampering, store logs off-site, and integrate with SIEM tools for advanced correlation and rapid incident identification
- establish baselines for normal network behavior and utilize security appliances to alert on deviations
- investigate any configuration modifications or alterations to network devices outside of the change management process

5 References

Number	Reference
1	Joint Guidance on Enhanced visibility and hardening for communications infrastructure https://www.cyber.gc.ca/en/news-events/joint-guidance-enhanced-visibility-hardening-communications-infrastructure
2	Security considerations for edge devices (ITSM.80.101) https://www.cyber.gc.ca/en/guidance/security-considerations-edge-devices-itsm80101
3	Government of Canada Patch Management Guidance https://www.canada.ca/en/government/system/digital-government/online-security-privacy/patch-management-guidance.html
4	Rethink your password habits to protect your accounts from hackers (ITSAP.30.036) Rethink your password habits to protect your accounts from hackers (ITSAP.30.036)
5	Best practices for passphrases and passwords (ITSAP.30.032) Best practices for passphrases and passwords (ITSAP.30.032)
6	Top 10 IT security actions: No.5 segment and separate information (ITSM.10.092) Top 10 IT security actions: No. 5 segment and separate information – ITSM.10.092
7	Routers cyber security best practices (ITSAP.80.019) Routers cyber security best practices - ITSAP.80.019
8	Secure your accounts and devices with multi-factor authentication (ITSAP.30.030) Secure your accounts and devices with multi-factor authentication (ITSAP.30.030)
9	NSA Publishes Best Practices for Selecting Cisco Password Types (2022) NSA Publishes Best Practices for Selecting Cisco Password Types (2022)
10	National Cyber Threat Assessment 2025-2026 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026