H E A D Q U A R T E R S
ARMED FORCES OF THE PHILIPPINES CYBER COMMAND
Camp General Emilio Aguinaldo, Quezon City

CYBERSECURITY BULLETIN 2025-02

Chinese Hackers Breach Cisco Devices in Global Telecom Attacks

Overview

A newly uncovered cyber espionage campaign led by the Chinese state-sponsored hacking group Salt Typhoon (Red Mike) has compromised vulnerable Cisco devices worldwide. Telecommunications providers across multiple countries, including the United States, the United Kingdom, and South Africa, have been targeted, posing significant national security risks.

Between December 2024 and January 2025, cybersecurity researchers at Recorded Future's Insikt Group tracked Salt Typhoon's activities and identified attempts to exploit over 1,000 Cisco devices globally.

Targeted Sectors and Locations

- Telecommunications providers were the primary targets.
- University networks in Argentina, Bangladesh, Indonesia, Malaysia, Mexico, the Netherlands, Thailand, the U.S., and Vietnam were also affected.
- Institutions such as UCLA and TU Delft were likely targeted due to their research in telecommunications, engineering, and technology.

Exploited Vulnerabilities

The attack leveraged two critical privilege escalation vulnerabilities in Cisco IOS XE software:

1. **CVE-2023-20198** – Exploited via the web user interface (UI), allowing unauthorized privileged account creation.

2. **CVE-2023-20273** – Used to escalate privileges to root access, enabling manipulation of device configurations and persistent access.

Tactics and Techniques

- **Initial Access**: Exploiting **CVE-2023-20198** to gain unauthorized entry.
- **Privilege Escalation**: Utilizing **CVE-2023-20273** for full control.
- **Persistence**: Deploying a **Generic Routing Encapsulation (GRE) tunnel** for covert data exfiltration and long-term network monitoring.

Strategic Intelligence Operations

Salt Typhoon's activities highlight China's broader cyber strategy to infiltrate critical infrastructure. Persistent access to telecom networks allows adversaries to intercept sensitive communications, manipulate data traffic and disrupt operations during geopolitical crises. Some of their confirmed victims are the U.S.-based affiliate of a major U.K. telecommunications provider, a South African telecommunications company, a large Thai telecommunications provider, a U.S. internet service provider (ISP) and an Italian ISP.

In December 2024, Salt Typhoon also conducted reconnaissance against Myanmar-based telecom provider Mytel, scanning for vulnerabilities in its infrastructure.

Recommendations

The Salt Typhoon campaign underscores the persistent threats posed by state-sponsored cyber adversaries. Organizations, particularly those in critical infrastructure sectors, must take immediate action to mitigate risks. The following are the recommended security measures for this matter:

1. **Patch Management**

    - Apply the latest **Cisco IOS XE updates** addressing **CVE-2023-20198** and **CVE-2023-20273**.
    - Implement an **automated patching system** to address vulnerabilities promptly.

2. **Network Hardening**

    - Restrict **web UI access** to trusted IP ranges.
    - Implement **multi-factor authentication (MFA)** for administrative accounts.
    - Disable unused **remote access services** to minimize attack surfaces.

3. **Intrusion Detection and Response**

    - Deploy **advanced intrusion detection systems (IDS)** to monitor anomalous activity.
    - Utilize **threat intelligence feeds** to detect indicators of compromise (IOCs) related to Salt Typhoon.

- Conduct regular **penetration testing** to identify exploitable vulnerabilities.

4. **Data Security and Encryption**

    - Encrypt sensitive communications to **prevent eavesdropping**.
    - Implement **zero-trust security models**, requiring continuous verification of user and device identities.

5. **Incident Response Preparedness**

    - Establish a cyber incident response team (CIRT) trained to handle state-sponsored attacks.
    - Develop and test a cybersecurity incident response plan with tabletop exercises.

6. **Government and Industry Collaboration**

    - Share threat intelligence with government agencies and private sector partners.
    - Participate in cybersecurity information-sharing initiatives to enhance situational awareness.

By adopting these best practices, organizations can enhance resilience against state-sponsored cyber threats and protect critical infrastructure from persistent espionage campaigns.

Reference: *https://cyberinsider.com/chinese-hackers-breach-cisco-devices-in-global-telecom-attacks/*