Title: Public Report on Unaddressed Network Exposure in Indian Telecom Infrastructure

Author: Subodh Deshpande
Date: May 2025

---

1. Introduction

In the course of independent threat research, I identified a critical exposure affecting the network infrastructure of a major Indian telecom provider. Specifically, I discovered **four separate IP addresses**, each tied to a distinct Layer 3 (L3) switch within the provider's network. These devices were:

- Running **outdated Cisco IOS XE firmware** vulnerable to known remote code execution (RCE) exploits.
- Broadcasting sensitive configuration and operational data over the internet via SNMP.
- Actively establishing outbound **SSH connections to IP addresses hosted on Alibaba Cloud infrastructure in China.**

Despite reporting this issue through proper responsible disclosure channels — including CERT-In, NCIIPC, and directly to the telecom company — no mitigation action has been observed, and the affected infrastructure remains exposed as of the date of this publication.

This report provides a clear overview of the threat, what was discovered, and why the absence of a response raises serious concerns about the handling of security disclosures involving critical national infrastructure.

---

2. Why This Matters: The Role of Layer 3 Switches

A Layer 3 (L3) switch is not just a fancy router. It serves as a **traffic controller** for thousands—sometimes millions—of users in a regional telecom network. It routes, filters, and manages network traffic at the backbone level.

If such a device is compromised:

- Data can be silently siphoned.
- Network traffic can be monitored, redirected, or interrupted.
- Attackers can use it as a pivot to move laterally across telecom infrastructure.

This is the kind of hardware a state-sponsored attacker would love to own.

---

3. What I Found

In April 2025, during independent research into Chinese threat groups, I discovered:

- **Four IP addresses** belonging to Indian Private telecom infrastructure.
- Devices running **outdated Cisco IOS XE firmware** known to be vulnerable to Remote Code Execution (RCE).
- **SNMP services exposed to the public internet**, broadcasting internal data such as OS version, system uptime, and routing configurations.
- On the private telecom IPs: open **Cisco Smart Install** ports (4786) with known RCE vulnerabilities.
- Most critically: **active SSH connections** from these devices to IP addresses hosted on **Alibaba Cloud in China**.

This pattern of behavior matches techniques used by state-linked threat actor groups, including the Typhoon family.

---

4. Attribution and Context

While I cannot claim conclusive attribution without full internal logs or malware samples, the activity observed is consistent with known tactics used by the Typhoon family:

- Targeting edge networking gear (especially Cisco and Fortinet)
- Using exposed management ports (SNMP, Smart Install)
- Maintaining covert remote access via SSH, often using Chinese cloud providers

These tactics have been observed in prior attacks on U.S. and Asia-Pacific telecom infrastructure.

---

5. Timeline of Events

- **April 21, 2025:** Issue reported to CERT-In and the affected private telecom company.
- **April 23, 2025:** CERT-In responds with incident ID.
- **April 30, 2025:** Email sent to the company regarding lack of response.
- **May 2, 2025:** Report submitted to NCIIPC.
- **May 3, 2025:** NCIIPC acknowledges the issue.

- **May 16, 2025:** No communication received from the telecom company; issue remains unaddressed.

---

6. Why I'm Going Public

I had hoped for a simple, responsible process: Report the issue, let the experts fix it, and move on.

That didn't happen.

- The devices are **still leaking sensitive information**.
- SSH connections to Chinese infrastructure **are still active**.
- The telecom provider **has not responded**, even after follow-up warnings.

As someone who values responsible disclosure and national security, I believe it is now in the public interest to raise awareness. This report has been redacted to prevent misuse, but the threat is real and urgent.

---

7. Closing Note

I am not affiliated with any organization. I am an independent researcher who believes defenders should speak up when they see something wrong.

If this issue receives the attention it deserves, I will consider this disclosure successful.

Disclaimer: All scans and findings were performed using publicly available tools and non-intrusive methods. No unauthorized access was attempted. This report is shared in good faith to encourage security, accountability, and action.