Canada says Salt Typhoon hacked telecom firm via Cisco flaw

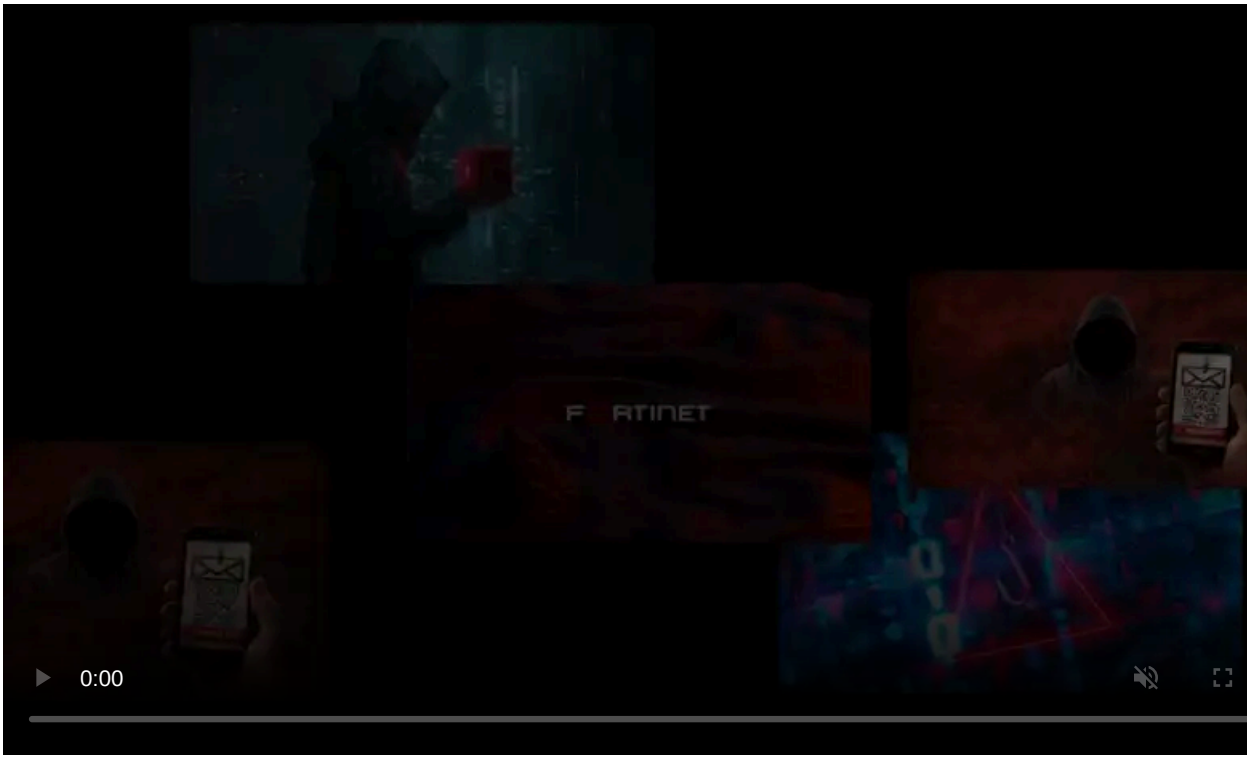
By Bill Toulas

Published: 2025-06-23 · Archived: 2026-04-05 23:21:21 UTC

The Canadian Centre for Cyber Security and the FBI confirm that the Chinese state-sponsored 'Salt Typhoon' hacking group is also targeting Canadian telecommunication firms, breaching a telecom provider in February.

During the February 2025 incident, Salt Typhoon exploited the CVE-2023-20198 flaw, a critical Cisco IOS XE vulnerability allowing remote, unauthenticated attackers to create arbitrary accounts and gain admin-level privileges.

The flaw was first disclosed in October 2023, when it was reported that threat actors had exploited it as a zero-day to hack over 10,000 devices.


F RTINET
0:00

Despite a significant period having passed, at least one major telecommunications provider in Canada still hadn't patched, giving Salt Typhoon an easy way to compromise devices.

"Three network devices registered to a Canadian telecommunications company were compromised by likely Salt Typhoon actors in mid-February 2025," reads the bulletin.

"The actors exploited CVE-2023-20198 to retrieve the running configuration files from all three devices and modified at least one of the files to configure a GRE tunnel, enabling traffic collection from the network."

In October 2024, following Salt Typhoon breaches on multiple American broadband providers, the Canadian authorities flagged reconnaissance activity that targeted dozens of key organizations in the country.

No actual breaches were confirmed at the time, and despite the calls to elevate security, some critical service providers didn't take the required action.

The Cyber Centre notes that, based on separate investigations and crowd-sourced intelligence, activity likely tied to Salt Typhoon extends beyond the telecommunications sector, targeting multiple other industries.

In many cases, the activity is limited to reconnaissance, though the data stolen from internal networks can be used for lateral movement or supply chain attacks.

The Cyber Centre warned that the attacks against Canadian organizations "will almost certainly continue" over the next two years, urging critical organizations to protect their networks.

Telecommunication service providers who handle valuable data, such as call metadata, subscriber location data, SMS contents, and government/political communications, are prime targets for state-sponsored espionage groups.

Their attacks typically target edge devices at the network perimeter, routers, firewalls, and VPN appliances, while MSPs and cloud vendors are also targeted for indirect attacks on their customers.

The Cyber Centre's bulletin lists resources providing edge device hardening instructions for critical infrastructure operators.

Salt Typhoon attacks have impacted multiple telecom companies in dozens of countries, including AT&T, Verizon, Lumen, Charter Communications, Consolidated Communications, and Windstream.

Last week, Viasat also confirmed that Salt Typhoon had breached them, but customer data was not impacted.

Source: https://www.bleepingcomputer.com/news/security/canada-says-salt-typhoon-hacked-telecom-firm-via-cisco-flaw/