IMPORTANT CYBERSECURITY NEWS: CISCO CONFIRMS SALT TYPHOON EXPLOITED CVE-2018-0171 TO TARGET U.S. TELECOM NETWORKS

Vairav Cyber Security News Report

Date: 2025-02-24

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: mail@vairavtech.com

EXECUTIVE SUMMARY

A recent cybersecurity incident involving U.S. telecommunications companies has resulted in the compromise of network infrastructure. The Chinese state-sponsored threat actor known as Salt Typhoon exploited a known vulnerability, CVE-2018-0171, and utilized stolen credentials to infiltrate these networks. Attackers maintained prolonged access, with one instance persisting undetected for over three years. This breach underscores the importance of promptly addressing known vulnerabilities and implementing robust credential management practices to protect critical infrastructure.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: Salt Typhoon exploited the CVE-2018-0171 vulnerability in Cisco's Smart Install feature and used stolen login credentials to gain unauthorized access to U.S. telecommunications networks. Salt Typhoon is a sophisticated and well-funded Advanced Persistent Threat (APT) group linked to China's Ministry of State Security. They employ living-off-the-land techniques, using existing network tools to move laterally and avoid detection.

Identification: The attack was identified through security investigations conducted by Cisco's threat intelligence unit, Talos. Their analysis revealed the prolonged presence of Salt Typhoon within the affected networks.

Threat Actor: The attack has been attributed to Salt Typhoon, an APT group associated with China's state-sponsored cyber espionage activities.

Affected Entities/Industries: Major U.S. telecommunications companies were the primary targets of this campaign. The attackers aimed to infiltrate and persist within critical communication infrastructures.

Potential Impact: The breach poses significant risks, including potential exposure of sensitive communications data, operational disruptions, financial losses, and reputational damage to the affected companies. The attackers' prolonged presence indicates a high level of access that could be leveraged for extensive data exfiltration and further exploitation.

Exploitation Methods: The attackers exploited the CVE-2018-0171 vulnerability in Cisco's Smart Install feature to gain initial access. They also obtained and utilized legitimate login credentials, possibly through capturing SNMP, TACACS, and RADIUS traffic to enumerate additional credential details. Their tactics included creating local accounts, enabling Guest Shell access, and facilitating remote access via SSH. A custom utility named JumbledPath was used to execute packet captures on remote Cisco devices, aiding in obfuscation and persistence.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Apply patches for CVE-2018-0171 and ensure all systems are updated to address known vulnerabilities.
- Conduct a comprehensive audit of user accounts and credentials; reset passwords and implement multi-factor authentication (MFA) where possible.
- Review and restrict network device configurations to limit unnecessary access and services.

Security Best Practices

- Regularly update and patch all software and hardware components.
- Implement strong password policies and enforce MFA across all access points.
- Conduct continuous network monitoring to detect and respond to suspicious activities promptly.
- Educate employees about phishing and other social engineering attacks to prevent credential compromise.

For Advanced Security Teams

- Deploy intrusion detection and prevention systems (IDPS) to identify and block malicious activities.
- Utilize network segmentation to isolate critical systems and limit lateral movement within the network.
- Perform regular security assessments and penetration testing to identify and remediate potential vulnerabilities.
- Develop and test incident response plans to ensure readiness against potential breaches.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/02/cisco-confirms-salt-typhoon-exploited.html
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com