BREAKING CYBERSECURITY NEWS: HACKERS ACTIVELY SCANNING FOR JUNIPER'S SESSION SMART ROUTERS USING DEFAULT CREDENTIALS

Vairav Cyber Security News Report

Date: April 04, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Between March 23 and 28, 2025, cybersecurity analysts observed a sudden surge in coordinated scanning activity targeting Juniper Networks' **Session Smart Router (SSR)** platform. Approximately 3,000 unique IP addresses were detected attempting to log in using the default factory credentials.

This spike in activity is likely associated with the **Mirai botnet**, which specializes in exploiting default passwords to conscript devices into distributed denial-of-service (DDoS) botnets. The attack campaign appears to be automated, targeting SSH access with credential-stuffing techniques, and may also be probing unpatched devices vulnerable to a critical SSR vulnerability (CVE-2025-21589). The graph in the original report highlights the synchronized rise and fall in login attempts using "t128" and "128tRoutes," clearly indicating the use of automated attack tools.

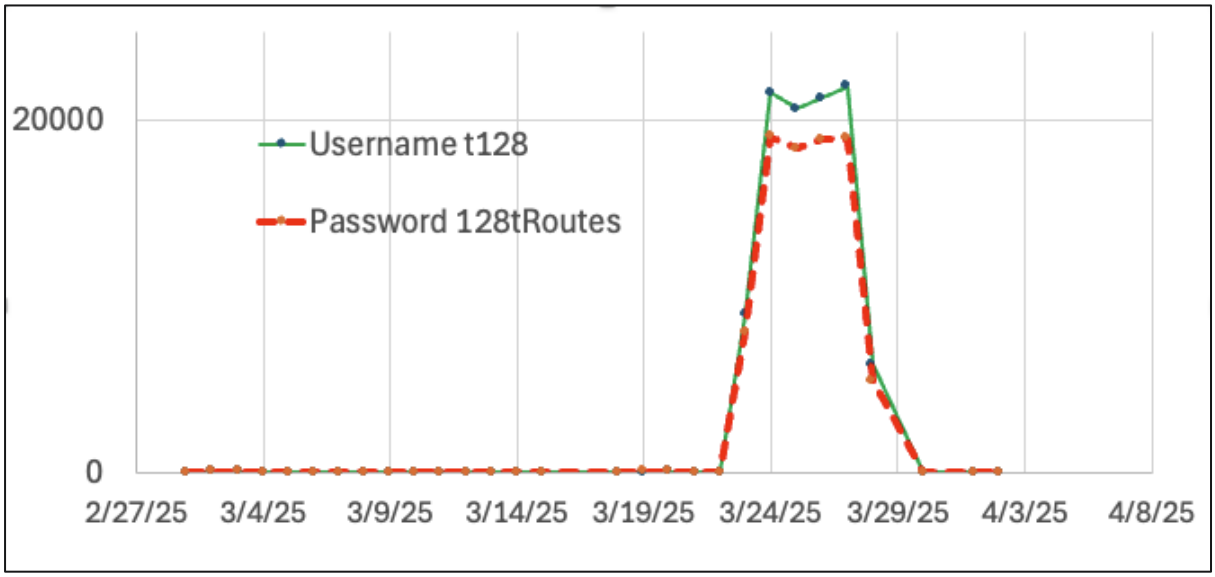

Figure 1: Graph representing rise and fall synchronization in login attempts

INCIDENT ANALYSIS

- **Attack Window:** March 23–28, 2025
- **Target:** Juniper Session Smart Routers (SSR)
- **Attack Method:** Credential stuffing using default logins
- **Credentials Used:**

  Username: t128 | Password: 128tRoutes

  Username: root | Password: 128tRoutes

- **Tools Involved:** Likely Mirai botnet malware
- **Purpose:** Device takeover for botnet recruitment (DDoS, scanning, lateral movement)
- **Observed by:** SANS Institute
- **Historical Link:** Juniper's 2020 acquisition of 128 Technology'

The incident highlights the risks of leaving default settings unchanged and underscores the importance of routine hardening and timely patch management. Organizations using Juniper SSR systems should act immediately to secure their devices, as exposed systems risk being compromised and used in broader malicious operations.

CVE DETAILS:

CVE-2025-21589: Juniper SSR Authentication Bypass Vulnerability

Description: A critical vulnerability in Juniper's Session Smart Router (SSR) allowed attackers to bypass authentication and gain administrative control of the device via specially crafted SSH or web requests.

Impact: Unauthenticated remote access, administrative takeover, system modification, botnet infection potential.

CVSS Score: 9.8 (Critical)

Affected Products:

- Juniper Session Smart Router (SSR)
- Juniper Session Smart Conductor
- Juniper WAN Assurance Managed Routers

Affected Versions:

- from 5.6.7 up to (but not including) 5.6.17
- 6.0.8 through 6.1.12-lts
- 6.2.8-lts
- 6.3.3-r2

Exploitation: Although Juniper initially reported no evidence of exploitation, the surge in scanning and targeting behavior indicates a possible shift from reconnaissance to active exploitation, especially in systems where vulnerability remains unpatched, and default credentials are still in place.

RECOMMENDED ACTIONS

- **Change Default Credentials Immediately:** Replace both root and t128 account passwords with strong, unique alternatives.
- **Patch Devices:** Apply the latest available firmware and security patches from Juniper addressing CVE-2025-21589.
- **Restrict Remote Access:** Limit SSH and management interface exposure to internal IPs or secure VPNs only.
- **Monitor for Indicators of Compromise:** Watch for repeated SSH login attempts, scanning behavior, or traffic to known Mirai command-and-control infrastructure.
- **Reimage if Compromised:** Juniper recommends a full reimage of any potentially affected devices, as attacker modifications may be difficult to detect or reverse.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

https://cybersecuritynews.com/hackers-scanning-junipers-smart-router/

https://isc.sans.edu/diary/31824

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