BREAKING CYBERSECURITY NEWS: ALLEGED ZERO-DAY REMOTE CODE EXECUTION VULNERABILITY IN TP-LINK ROUTERS

Vairav Cyber Security News Report

Date: March 7, 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

A new remote code execution (RCE) exploit targeting TP-Link routers, dubbed "JumboJet TP-Link RCE Exploit," has surfaced on a dark web marketplace. This exploit allegedly allows attackers to gain full control over vulnerable TP-Link routers, enabling remote execution, auto-spreading, and data exfiltration. It leverages a command injection vulnerability in the LuCI web interface (depending on firmware versions), providing persistent backdoor access. Cybercriminals are actively selling this exploit, emphasizing its stealth and efficiency. Organizations using TP-Link routers should take immediate action to assess and mitigate potential vulnerabilities.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: The "JumboJet TP-Link RCE Exploit" is a zero-day vulnerability allowing remote code execution on TP-Link routers. The exploit allegedly automates large-scale attacks by injecting malicious payloads via a command injection vulnerability in the LuCI web interface, establishes a persistent backdoor, disables firewalls, and exfiltrates sensitive data such as router IPs, credentials, and Wi-Fi settings to an attacker-controlled server. The exploit spreads laterally by scanning for TP-Link routers with default credentials (admin:admin) and compromising them and the payload encrypts its backdoor communications using AES-256 for stealth and persistence. The base script is being sold for $1,000, while the base script with an additional month of support is priced at $2,000.

Affected Entities/Industries: Users and businesses utilizing TP-Link routers, particularly those running LuCI-based firmware along with industries relying on TP-Link networking equipment for home and office infrastructure are the risk. The risk extends to ISPs and enterprises offering TP-Link devices to customers.

Potential Impact:

- Unauthorized access to router configurations and credentials, leading to network compromise.

- Potential data breaches if attackers access internal systems through infected routers.
- Disruption of business operations and potential legal/regulatory implications

Exploitation Methods:

- Command injection vulnerability in LuCI web interface (firmware-dependent).
- Automated credential stuffing attack against routers using default credentials.
- Persistence via cron jobs and hidden processes.
- Encrypted backdoor for continued remote access.
- Data exfiltration to attacker-controlled servers.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Update TP-Link router firmware to the latest available version.
- Disable remote management features if not necessary.
- Change default credentials and enforce strong passwords.

Security Best Practices

- Monitor network traffic for unusual activity from TP-Link devices.
- Implement network segmentation to prevent lateral movement.
- Regularly back up router configurations and settings.

For Advanced Security Teams

- Conduct penetration testing on TP-Link routers to identify potential vulnerabilities.
- Use threat intelligence feeds to track related dark web activity.
- Deploy intrusion detection/prevention systems (IDS/IPS) to monitor unauthorized access attempts.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://breachforums.st/Thread-SELLING-JumboJet-TP-Link-RCE-Exploit-0-Day-Private-0-day?highlight=JumboJet

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