DRAGONFORCE RANSOMWARE EXPLOITS SIMPLEHELP VULNERABILITIES IN MSP SUPPLY CHAIN ATTACK

Vairav Cyber Security News Report

Date: May 30, 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

The DragonForce ransomware group has executed a targeted **supply chain attack** on a Managed Service Provider (MSP), exploiting flaws in the **SimpleHelp Remote Monitoring and Management (RMM)** platform. The attack involved the exploitation of three CVEs: **CVE-2024-57726**, **CVE-2024-57727**, and **CVE-2024-57728**, to gain unauthorized access and push ransomware to multiple downstream customer endpoints.

Data exfiltration and ransomware deployment were carried out across client environments, followed by **double-extortion tactics**. The incident underscores the growing risk of RMM abuse and the evolution of ransomware operations into **cartel-like affiliate models**, with DragonForce seeking dominance post-LockBit's disruption.

INCIDENT DETAILS

1. **Initial Access:** Threat actors infiltrated an MSP's SimpleHelp RMM platform by exploiting known vulnerabilities disclosed in January 2025. The flaws enabled unauthorized remote access and code execution.
2. **Attack Vector:** A malicious SimpleHelp installer was pushed via the MSP's legitimate SimpleHelp instance, triggering further compromise of customer endpoints.
3. **Post-Exploitation Activity:**
   - Reconnaissance across customer environments (device names, configurations, user details).
   - Exfiltration of sensitive data.
   - Deployment of ransomware payloads using the MSP's infrastructure.
4. **Dwell Time:** The attackers persisted in the environment for nine days before attempting encryption, allowing for extensive lateral movement and data theft.

CVE DETAILS

CVE-2024-57726: Authentication Bypass Vulnerability

Description: A flaw in SimpleHelp RMM's authentication mechanism allows an attacker to bypass login under specific conditions.

Impact: An attacker may gain unauthorized access to the RMM system, potentially accessing sensitive systems and operations without credentials.

CVSS Score: 8.6 (High)

CVE-2024-57727: Remote Command Execution Flaw

Description: A vulnerability in the SimpleHelp RMM backend allows remote attackers to execute arbitrary system commands without proper authorization.

Impact: Enables remote code execution (RCE), which can lead to full system compromise.

CVSS Score: 9.1 (Critical)

CVE-2024-57728: Privilege Escalation via Local Misconfiguration

Description: Improper local configuration in SimpleHelp RMM could be exploited by a local user to elevate privileges to an administrative level.

Impact: A low-privileged user could gain administrator-level access, leading to full control over the management system.

CVSS Score: 8.4 (High)

TACTICS AND THREAT ACTOR INSIGHTS:

- **DragonForce** is aggressively expanding with a **cartel model**, encouraging affiliate-based rebranding of its locker under different names.
- **Scattered Spider**, known for **identity-centric cloud intrusions**, may be collaborating or serving as an access broker in these campaigns.
- The operation overlaps with the defacement of rival groups like **BlackLock**, **Mamona**, and **RansomHub**, indicating turf wars among ransomware actors post-LockBit disruption.

VICTIMOLOGY

Sectors Impacted: Retail (UK), MSP clients across verticals.

TTPs observed:

- Supply chain compromises via RMM tools.
- Double extortion (data leak + ransomware).
- Use of virtual machines and remote access software to evade detection.
- Email bombing + vishing campaigns (3 AM ransomware overlap).
- Abuse of Microsoft Quick Assist for social engineering and access.

RECOMMENDED ACTIONS

- **Patch Immediately:** Apply fixes for CVE-2024-57726, CVE-2024-57727, and CVE-2024-57728 across all SimpleHelp instances.
- **Limit RMM Exposure:** Restrict RMM tools from external access. Implement strict access controls and MFA.
- **Monitor for Anomalies:** Watch for unusual installer deployments, elevated privilege creation, and outbound connections to untrusted IPs.
- **Harden Employee Awareness:** Educate staff on vishing, fake tech support, and email bombing tactics.
- **Restrict Remote Tools:** Block unauthorized use of remote desktop applications and virtual machine execution via policy enforcement.
- **Threat Hunt:** Perform proactive scanning for lateral movement, suspicious RMM activity, and unauthorized data access.

Strategic Takeaway

DragonForce represents a new wave of affiliate-driven ransomware**,** reshaping the ecosystem through decentralization, social engineering, and strategic alliances. Supply chain attacks through trusted IT providers are a critical risk vector. Organizations must reevaluate their vendor trust models, enforce strict RMM usage policies, and prepare for multi-stage, stealthy intrusions that blur the lines between ransomware and APT-style operations.

REFERENCES

https://thehackernews.com/2025/05/dragonforce-exploits-simplehelp-flaws.html

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