VPN Risk Report Finds More Than Half of Organizations Experienced a VPN-related Cyberattack in the Last Year

May 7, 2024

Zscaler ThreatLabz 2024 annual report reveals 78% of organizations plan to implement a Zero Trust strategy in the next 12 months in response to increasing exploits

- **VPN security concerns rise** as 91% of respondents express concerns about VPNs leading to a compromising breach
- **The survey identifies the top threats exploiting VPN** vulnerabilities to be ransomware (42%), other types of malware (35%), and DDoS attacks (30%)
- **Lateral movement is a top concern, as** reported by a majority of enterprises breached by VPN, demonstrating significant containment failures

SAN JOSE, Calif., May 07, 2024 (GLOBE NEWSWIRE) -- Zscaler, Inc. (NASDAQ: ZS), the leader in cloud security, today announced the release of the 2024 ThreatLabz VPN Risk Report. The study, reviewed by Cybersecurity Insiders, surveyed over 600 professionals across the security, IT, and networking sectors. It found that 56% of organizations have been targets of cyberattacks exploiting VPN security vulnerabilities in the last year. These incidents underscore the growing imperative to move away from traditional perimeter-based defenses towards a more robust Zero Trust architecture.

This shift to Zero Trust has gained momentum following recent high-profile breaches and critical vulnerabilities with VPNs from two large vendors:

- Ivanti (CVE-2023-46805 and CVE-2024-21887) - Remote attackers were able to perform authentication bypass and remote command injection exploits.
- Palo Alto Networks OS vulnerability (CVE-2024-3400) - Unauthenticated users exploited the security vendor's operating system to infiltrate the network. As a result, the vulnerability received the maximum severity score of 10.0.

The Ivanti zero-day vulnerabilities even led the Cybersecurity and Infrastructure Security Agency (CISA) to issue an emergency directive for federal agencies to immediately sever connections with the compromised VPN devices.

VPN security challenges
VPNs have traditionally facilitated remote enterprise access to networks, yet the growing scale and complexity of cyber threats targeting these networks remain a significant concern for security teams. Among those surveyed, 91% voiced apprehension regarding VPNs as weak entry points in their IT infrastructure, highlighted by recent breaches that exposed the dangers of relying on outdated or unpatched VPN infrastructure.

"Over the past year, numerous critical VPN vulnerabilities have served as successful entry points for attacks on large enterprises and federal entities," said Deepen Desai, CSO at Zscaler. "Considering these repeated outcomes, it's crucial for enterprises to anticipate that threat actors will increasingly exploit these legacy, internet-exposed assets — appliances and virtual — that enable them to easily navigate laterally across traditional flat networks. It is essential to transition to a Zero Trust architecture, which significantly reduces the attack surface by eliminating legacy technologies like VPNs and Firewalls, enforces consistent security controls with TLS inspection, and limits the blast radius with segmentation & deception, thereby preventing damaging breaches."

Key VPN vulnerability exploits
The report identifies ransomware attacks (42%), malware infections (35%), and DDoS attacks (30%), as the top threats exploiting VPN vulnerabilities. These statistics emphasize the extensive risks organizations face due to the inherent weaknesses in traditional VPN architectures, reinforcing the need for a shift to Zero Trust architecture. Notably, the report revealed that 78% of surveyed organizations plan to actively implement Zero Trust strategies within the next 12 months. Additionally, 62% of enterprises acknowledge that VPNs go against the principles of Zero Trust and that even delivering VPNs through the cloud does not constitute a Zero Trust architecture.

Stop the spread
Among enterprises who were breached via VPN vulnerabilities, a majority of impacted enterprises say threat actors moved laterally on the network, demonstrating significant containment failures after the initial point of compromise. To help minimize the blast radius and mitigate risk from VPN vulnerabilities, Zscaler strongly urges the adoption of a Zero Trust architecture. A Zero Trust architecture will help enterprises:

- **Minimize the attack surface** by making apps invisible to the internet, making them more difficult for attackers to discover and target
- **Prevent compromise** with inline traffic and content inspection to detect and block malicious activity and shield resources from unauthorized access or data exfiltration
- **Eliminate lateral movement** by segmenting and connecting users directly to applications instead of the network, thus limiting an attackers' opportunities for unauthorized access and lateral spread

To learn more about the risks VPNs pose to the enterprise, download the Zscaler ThreatLabz 2024 VPN Risk Report with Cybersecurity Insiders at: www.zscaler.com/campaign/threatlabz-vpn-risk-report

Methodology
The VPN Risk Report surveyed more than 600 security, IT, and networking professionals.

About Zscaler
Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SASE-based Zero Trust Exchange™ is the world’s largest in-line cloud security platform.

Media Contact:
Zscaler PR
press@zscaler.com