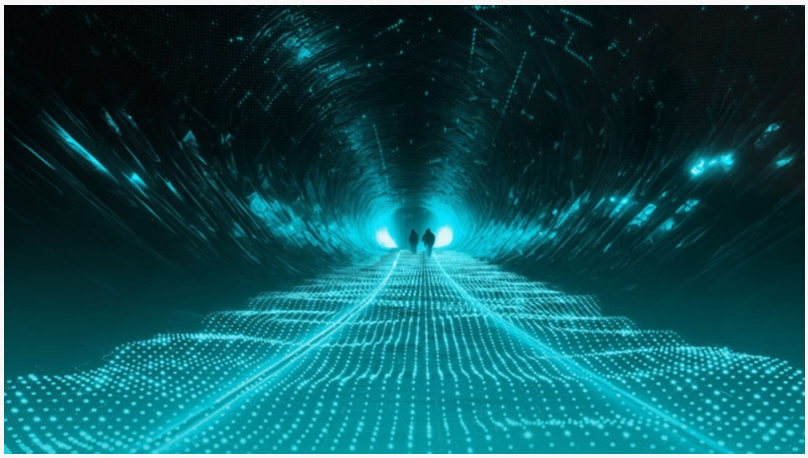
Vulnerabilities in business VPNs under the spotlight



DUBAI, UNITED ARAB EMIRATES, March 10, 2024 /EINPresswire.com/ -- Márk Szabó, PR and Security Writer at ESET explains that as adversaries increasingly set their sights on vulnerable enterprise VPN software to infiltrate corporate networks, concerns mount about VPNs themselves being a source of cyber risk.

Virtual Private Network (VPN) services have emerged as essential tools for modern businesses in recent years, doubly so since helping save the day for many of them amid the pandemic-fueled, pell-mell rush to remote work in 2020. By creating an encrypted tunnel for corporate data traveling between company networks and employee devices, VPNs help secure sensitive information without compromising employee productivity or crippling companies' mission-critical operations. As many organizations have since settled into a hybrid workplace model that mixes in-office and on-the-go work, remote access VPNs have remained a staple in their network connectivity and security toolkits.

On the other hand, VPNs have also come under increasing scrutiny due to a surge in security vulnerabilities and exploits targeting them, sometimes even before patches are rolled out. Since VPNs potentially represent the keys to the corporate kingdom, their appeal to nation-state actors and cybercriminals alike is undeniable. Adversaries are dedicating substantial resources to scouring for weak points in corporate software stacks, which exerts further pressure on organizations and underscores the importance of robust risk mitigation practices.

In an era where the mass exploitation of security loopholes, large-scale supply-chain attacks, and other breaches of corporate defenses are increasingly common, concerns are mounting not only about the ability of VPNs to help safeguard corporate data against bad actors, but also about this software itself being yet another source of cyber-risk.

This begs the question: could business VPNs be a liability that increases your organization's

attack surface?

Keys to the kingdom

A VPN routes the user's traffic through an encrypted tunnel that safeguards the data against prying eyes. The main raison d'etre of a business VPN is to create a private connection over a public network, or the internet. In so doing, it gives a geographically dispersed workforce access to internal networks as if they were sat at their office desks, essentially making their devices part of the corporate network.

But just like a tunnel can collapse or have leaks, so can a vulnerable VPN appliance face all manner of threats. Out-of-date software is often a reason many organizations fall victim to an attack. Exploitation of a VPN vulnerability can enable hackers to steal credentials, hijack encrypted traffic sessions, remotely execute arbitrary code and give them access to sensitive corporate data. This VPN Vulnerability Report 2023 provides a handy overview of VPN vulnerabilities reported in recent years.

Indeed, just like any other software, VPNs require maintenance and security updates to patch vulnerabilities. Businesses seem to be having a hard time keeping up with VPN updates, however, including because VPNs often have no planned downtimes and are instead expected to be up and running at all times.

Ransomware groups are known to often target vulnerable VPN servers, and by gaining access at least once, they can move around a network to do whatever they please, such as encrypting and holding data for ransom, exfiltrating it, conducting espionage, and more. In other words, the successful exploitation of a vulnerability paves the way for additional malicious access, potentially leading to a widespread compromise of the corporate network.

Cautionary tales abound

Recently, Global Affairs Canada has begun an investigation into a data breach caused by a compromise of its VPN solution of choice, which had been ongoing for at least a month. Allegedly, hackers gained access to an undisclosed number of employee emails and various servers that their laptops had connected to from December 20th, 2023, until January 24th, 2024. Needless to say, data breaches come with immense costs – $4.45 million on average, according to IBM's Cost of a Data Breach 2023 report.

In another example, back in 2021 Russia-aligned threat actors targeted five vulnerabilities in corporate VPN infrastructure products, which necessitated a public warning by the NSA urging organizations to apply the patches as soon as possible or else face the risk of hacking and espionage.

Another worry is design flaws that aren't limited to any given VPN service. For example, TunnelCrack vulnerabilities, unearthed by researchers recently and affecting many corporate and consumer VPNs, could enable attackers to trick victims into sending their traffic outside the

protected VPN tunnel, snooping on their data transmissions.

Critical security updates are required to plug these kinds of security loopholes, so staying on top of them is a must. So is employee awareness, as another traditional threat involves bad actors using deceptive websites to trick employees into surrendering their VPN login credentials. A crook can also steal an employee's phone or laptop in order to infiltrate internal networks and compromise and/or exfiltrate data, or quietly snoop on the company's activities.

Securing the data

A business should not rely solely on their VPN as a means to protect their employees and internal information. A VPN does not replace regular endpoint protection, nor does it replace other authentication methods.

Consider deploying a solution that can help with vulnerability assessment and patching as the importance of staying on top of security updates issued by software makers, including VPN providers, cannot be stressed enough. In other words, regular maintenance and security updates are one of the best ways of minimizing the odds of a successful cyber-incident.

Importantly, take additional measures to harden your VPN of choice against compromise. The United States' Cybersecurity and Infrastructure Security Agency (CISA) and National Security Agency (NSA) have a handy brochure that outlines various precautions that do just that. This includes shrinking the attack surface, using a strong encryption to scramble the sensitive corporate data, robust authentication (like an added second factor in the form of a one-time code) and VPN use monitoring. Use a VPN that complies with industry standards and is from a reputable vendor with a proven track record in following cybersecurity best practices.

No VPN software guarantees perfect protection and a business would be ill-advised to rely solely on it for access management. Organizations can also benefit from exploring other options to support a distributed workforce, such as the zero trust security model that relies on continuous authentication of users, as well as other controls, which include continuous network monitoring, privileged access management and secure multi-layered authentication. Add endpoint detection and response to the mix, as that can, among other things, shrink the attack surface, and its AI-based threat detection capabilities can automatically highlight suspicious behaviour.

Additionally, consider the VPN security you have or want. This means that VPNs can differ in what they offer, as there is a lot more under the surface than just creating a simple connection to a server since it might also include various additional security measures. And VPNs can also differ in how they handle user access, one might require constant input of credentials, while another could be a one-and-done thing.

Parting thoughts

While VPNs are often a crucial component for secure remote access, they can be – especially in the absence of other security practices and controls – juicy targets for attackers looking to break

into corporate networks. Various advanced persistent threat (APT) groups have recently weaponized known vulnerabilities in VPN software to pilfer user credentials, execute code remotely and extract corporate crown jewels. Successful exploitation of these vulnerabilities typically paves the way for additional malicious access, potentially leading to large-scale compromises of corporate networks.

As work patterns evolve, the demand for remote access persists, which underscores the ongoing importance of prioritizing the security of a dispersed workforce as a fundamental element within an organization’s security strategy.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here
