



Pulse Secure Zero Day



Overview

Threat actors that are likely backed by nation-states are exploiting a number of vulnerabilities in the Pulse Secure VPN. One of the vulnerabilities is a zero-day, which allows the attackers to bypass multi-factor authentication (MFA) protections that the affected organizations have in place. It appears that 12 malware families are exploiting these vulnerabilities. While it's not clear whether these families are directly related, experts say there are multiple actors at play. Once attackers exploit these vulnerabilities and bypass authentication, they install malware that persists through software updates and allow remote access and control through webshells.

Lookout Analysis

This incident exemplifies where VPN technology can fall short. VPNs enable whoever is connected to tunnel directly into their organization's infrastructure while assuming the user and device can be trusted. Once inside, users can move laterally within the network, which could be detrimental if an attacker exploits the VPN to do this. Zero Trust Network Architecture (ZTNA) helps organizations avoid the pitfalls of VPN. ZTNA continuously monitors the identity of those requesting access to your apps and provides dynamic identity and context-aware access to cloud data depending on the risk level of the user and device.

Recommendation for Lookout Admins

Security teams want to give employees enough data access to do their jobs, but not so much that they have access to everything. Lookout admins can implement Lookout ZTNA to mitigate the risk of unauthorized access and breaches caused by over-entitlement of services. This will also help bring the security benefits of SaaS applications to legacy, IaaS, and private apps to ensure all your corporate resources are properly secure.

Admins can also define context-aware adaptive access control policies to deliver Zero Trust access based on unique user and device identifiers. Lookout ZTNA also enables data loss prevention (DLP) and admins can leverage enterprise digital rights management (E-DRM) to automatically envelop data with advanced encryption based on its sensitivity.

Lookout Zero Trust Network Access (ZTNA)

Lookout ZTNA enables organizations to implement granular identity and context-aware access controls that deliver consistent security and use experience across on-premises, IaaS, and SaaS apps. Security teams can limit access only to those who need it, extend advanced security to legacy apps, and implement agentless access from any endpoint device.

[Click here to learn more about Lookout ZTNA](#)