THE
NATIONAL LAW REVIEW

VPN Packages Store Cookies Insecurely

Thursday, April 18, 2019

The Department of Homeland Security (DHS) issued a warning on April 15, 2019, entitled “VPN Applications Insecurely Store Session Cookies” (Vulnerability Note VU#192371) stating that “[M]ultiple Virtual Private Network (VPN) applications store the authentication and/or session cookies insecurely in memory and/or log files.”

The affected products identified by DHS are:

- Palo Alto Networks GlobalProtect Agent 4.1.0 for Windows and GlobalProtect Agent 4.1.10 and earlier for macOS0 (CVE-2019-1573)
- Pulse Secure Connect Secure prior to 8.1R14, 8.2, 8.3R6, and 9.0R2
- Cisco AnyConnect 4.7.x and prior

Robinson+Cole

Article By Robinson & Cole LLP
Linn F. Freedman
Data Privacy + Security Insider

Communications, Media & Internet
All Federal

According to US-CERT, “[I]f an attacker has persistent access to a VPN user’s endpoint or exfiltrates the cookie using other methods, they can replay the session and bypass other authentication methods. An attacker would then have access to the same applications that the user does through their VPN session.”

A patch is available for the Palo Alto products, but as of April 15, 2019, US-CERT was unaware of a patch for the Cisco product.

If your organization is using any of these products, or if you believe that your organization is vulnerable, US-CERT suggests that you contact CERT/CC at cert@cert.org with the affected products, version numbers, patch information, and self-assigned CVE.

Source URL: https://www.natlawreview.com/article/vpn-packages-store-cookies-insecurely