Authentication tool on many enterprise VPN applications that are bypassed by hackers

Security experts have recently discovered that many corporate VPN applications are developed by software companies like Palo Alto Networks, Pulse Secure, Cisco and F5 Networks that are hosting authentication cookies and session cookies. unsafe way of scene, capable of allowing an attacker to ignore the default authentication feature.

Security experts have recently discovered that many corporate VPN applications are developed by software companies like Palo Alto Networks, Pulse Secure, Cisco and F5 Networks that are hosting authentication cookies and session cookies. insecure, capable of allowing an attacker to ignore the default authentication feature.

1. Malware and user security bugs are found in top free VPN applications

The above information is given in the DHS / CISA report and notes the vulnerability issued by CERT / CC. In addition, as detailed in the Common Weakness Enumeration database in CWE-311, the application does not "encrypt sensitive or important information before storing or transmitting data" may allow attackers to It proceeded to block traffic data, read and inject code as well as malicious data into the system to perform a Man-in-the-Middle (MitM) attack.

In addition, a major announcement released on April 15 by the US Department of Homeland Security's National Security and Infrastructure Security Agency (CISA) also confirmed that an "attacker has can exploit this vulnerability to control the affected system ".

Meanwhile, the vulnerability note written by Carnegie Mellon University renowned security researcher Madison Oliver also said "if an attacker has continuous access to the endpoint of a VPN user or leaks." rustling cookies with many other methods, they can completely go back to the session and ignore the existing authentication methods.The attacker will then have access to the applications that the user does through the VPN session. mine".

1. 25% of "out-of-the-box" phishing emails are the default security of Office 365

Notice of CERT / CC is as follows:

The following applications and VPN application versions are storing unsafe cookies in log files:

1. *Palo Alto Networks GlobalProtect Agent 4.1.0 for Windows, GlobalProtect Agent 4.1.10 and earlier versions for macOS0 (CVE-2019-1573).*
2. *Previous Pulse Secure Connect Secure version 8.1R14, 8.2, 8.3R6 and 9.0R2.*

The following applications and application versions store unsafe cookies in memory:

1. *Palo Alto Networks GlobalProtect Agent 4.1.0 for Windows, GlobalProtect Agent 4.1.10 and earlier versions for macOS0 (CVE-2019-1573).*
2. *Previous Pulse Secure Connect Secure version 8.1R14, 8.2, 8.3R6 and 9.0R2.*
3. *Cisco AnyConnect 4.7.x and earlier versions.*

In addition, according to CERT / CC notes, "it is possible that this configuration is common to additional VPN applications", ie hundreds of VPN applications from a total of 237 providers on the market today. potentially affected by this disclosure vulnerability.

1. The hyperlink test command is being used by hackers to perform DDoS

While Check Point Software Technologies VPN applications and pfSense have been proven not to be vulnerable, two other large VPN service providers, Cisco and Pulse Secure, have yet to provide any feedback. about this vulnerability.

In a related move, Palo Alto Networks posted a security recommendation, which included more information about this CVE-2019-1573 security vulnerability, and also released GlobalProtect Agent version 4.1.1. for Windows users, and then GlobalProtect Agent 4.1.11 for macOS security updates.

On the other hand, F5 Networks has been "aware of unsafe memory storage since 2013" and decided not to patch this vulnerability, but instead provided the following solution as a means to minimize the impact for user:

"To minimize the impact of this vulnerability, you can use one-time password or two-factor authentication instead of a password-based authentication."

However, the unsafe log storage issue has also been patched by this publisher in the F5 Networks BIG-IP application since versions 12.1.3 and 13.0.1, released in 2017.

1. Reveal personal data of more than 1.3 million people from a vulnerability in web application

PulseSecure has also released a non-cyclical security recommendation regarding incorrect session cookie handling in some versions of the Pulse Desktop Client application and Pulse Connect Secure (for Network

Connect customers). The provider said that the patch versions of the Pulse Desktop Client or Pulse Connect Secure (for Network Connect customers) are available for download on the Pulse Secure Download Center.