FortiClient VPN successful Logging Blindspot

Fortinet VPN design flaws hides successful brute-force attacks

Overview

A design flaw in the Fortinet VPN server logging system can be leveraged to conceal a successful brute-force attack without alerting Incident Responders of the successful logon after a brute-force attempt.

Although the brute-force attempts will be detected, there will be no way of detecting if this resulted to a successful login, generating a false sense of security.

Flaw Explained

FortiClient VPN server stores login activity using a two-step process that consists of an authentication and an authorization stage.

A successful logon will only be recorded if the process passes both the authentication and authorization stages, otherwise it will be depicted as a failed logon.

With the flaw, an attacker devises a method to stop full login process (using a proxy tool such as *Burpe Suite*) after the authentication stage, allowing them to validate valid VPN credentials without logging in.

Risk Factor

The inability to log successful authentication at the authentication stage would allow an attacker to conduct brute-force attacks without detection of their successful attempts. An attacker with a bank of credentials could determine which credentials are valid without exposing compromised users.

The Incident Response (IR) team will not be able to identify the compromised credentials to initiate a call-to-action to reset the user's password. The attacker can leverage this gap to authenticate with the compromised credentials later or sell the credentials on the dark web.

Mitigation Strategies

FortiNet VPN users should implement additional security measures such as multi-factor authentication.

Allow for strict monitoring of authentication logs.

Log for "SSL tunnel shutdown" without a prior "SSL tunnel established" as this sequence may hint at validated but unutilized credentials.

Implementation of a Web Application Firewall (WAF) before the VPN server to detect this kind of attack.

Monitor for common attack tools such as Metasploit or Burpe suite or unusual behavior of OpenConnect leveraged in brute-force campaigns targeting FortiNet VPNs.

References:

https://pentera.io/blog/forticlient-vpn_logging-blind-spot-revealed/

https://www.bleepingcomputer.com/news/security/fortinet-vpn-design-flaw-hides-successful-brute-force-attacks/

Information Sharing

We encourage any organization or individual that has any information related to this incident to share it with us through our email info@serianu.com or landline; +254 771949475 to allow us to further analyze and detect future potential threats.