Health-ISAC™
Collaborating for Resilience in Healthcare

THREAT BULLETINS

Cisco Warns of Password Spray Attacks Against VPN Services on Cisco Secure Firewall Devices

○○○ TLP:WHITE

Apr 01, 2024

On March 26, 2024, Cisco released an advisory stating that its threat intelligence team, Cisco Talos, has observed a concerning uptick in password spray attacks against Remote Access Virtual Private Network (RAVPN) services on devices that use Cisco Secure Firewall. According to Cisco Talos, this activity is most likely associated with reconnaissance efforts.

To identify this activity in member environments, Cisco notes that a staggering amount of authentication requests in system logs are indicative of this activity. The organization has viewed instances of this campaign where hundreds of thousands of authentication requests were made. It has also been reported that this campaign is capable of making millions of requests for systems. Also, in this campaign, the username is always hidden in the logs until the no logging hide username command is configured on the Adaptive Security Appliance (ASA).

It is also important to note that an independent security researcher, Aaron Martin, has attributed this activity to the previously undocumented Brutus Botnet.

Reference(s)	Cisco, Security Affairs, Bleeping Computer, AnnoyedEngineer

Sources
https://www.cisco.com/c/en/us/support/docs/security/secure-firewall-threat-defense/221806-password-spray-attacks-impacting-custome.html
https://securityaffairs.com/161205/hacking/cisco-warns-password-spraying-attacks.html
https://www.bleepingcomputer.com/news/security/cisco-warns-of-password-spraying-attacks-targeting-vpn-services/
https://annoyed.engineer/2024/03/23/the-brutus-botnet/

Incident Date
Mar 30, 2024 (UTC)

Alert ID 6788b5d7

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.