News article

May 2024

Cisco Warns of Campaign Targeting VPN's

Cisco has warned organisations of a global brute force campaign targeting VPNs from Cisco, CheckPoint, Fortinet, SonicWall, and Ubiquiti.

Craig Archdeacon
Head of Cyber Assurance

Email craig.archdeacon@waterstons.com

What happened

Since March 18th, an increase in brute force password spray attacks targeting VPNs has been observed by security researchers at Cisco Talos. These involve threat actors using the same password for multiple usernames before trying a new password, relying on users using simple, or easy to guess, passwords for success.

The recent password spray attacks targeting VPNs, have been observed using both generic and valid usernames, with the latter likely obtained from publicly available data, gained previous data breaches, on the dark web.

It is not clear what the impact of this increase has been but, depending on what other security controls are in place, the increase in attacks could lead to account takeovers, account lockouts, or denial of service (DoS) for targeted services.

Wider implications

This latest campaign targeting VPNs and other internet-facing devices highlights the importance of secure configuration of internet connected devices. In many cases, these types of attacks can be prevented or mitigated by utilising devices' built-in security features, such as disabling web portals for VPNs if not required or implementing a maximum number of failed logins before lockout.

This secure configuration can also be supported by conditional access controls to reduce the chance of a successful login, regardless of whether they have a password. Location-based restrictions in particular can be extremely effective in reducing an account's exposure to this type of attack.

Organisations should:

- Ensure that all appliances such as VPNs are securely configured in accordance with the manufacturer's guidance, including disabling any unused services/features such as a VPN web portal.
- Ensure all accounts are protected by number matching MFA, and conditional access controls where available.
- Ensure that all publicly-facing services are regularly assessed to ensure they are required to be so in order to minimise a potential attack surface.
- Perform dark web monitoring to identify any credentials stolen in previous data breaches, either from the organisation itself or suppliers.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430