Cyber expert warns Derbyshire firms after global firewall password leak

derbyshiretimes.co.uk/your-world/derbyshire-cyber-expert-warns-firms-after-global-firewall-password-leak-8753113

Kevin Walker June 22, 2026

“The lesson here is not that cyber criminals only go after big brands. It is that attackers automate this work at huge scale”

A Chesterfield cyber security specialist is urging Derbyshire businesses, schools, charities and public sector organisations to check whether they may be affected by a global campaign targeting Fortinet firewalls and VPN gateways.

The National Cyber Security Centre, (NCSC), has issued advice following reports that Fortinet firewalls and VPN systems have been targeted, with some indication of possible impact in the UK.

A leaked database of credentials has been published following brute-force, dictionary and credential stuffing attacks against internet-facing FortiGate and VPN portals.

AI-generated illustration | Image supplied by Black Swan Cyber Security Solutions. AI-generated illustration.

Credential stuffing is when criminals use passwords stolen from one service and try them against another. It is one of the reasons reused passwords remain such a serious business risk.

Kevin Walker, founder of Black Swan Cyber Security Solutions in Chesterfield, said the warning should not be dismissed as a problem for large companies only.

He said: “When people hear names like Fortinet, they often assume this is only an enterprise issue. Firewalls and VPNs are used by organisations of all sizes, including small businesses, schools, care providers, charities and local councils.

“The firewall is often the front door to the network. If attackers get valid credentials, they may not need to ‘hack’ their way in. They can simply log in.”

Cyber security researchers have reported that the wider leak may include tens of thousands of Fortinet-related records worldwide. Global companies reportedly listed in analysis of the dataset include technology, telecoms, manufacturing, finance and consultancy organisations.

Kevin said the presence of household names should make smaller organisations pay attention, not assume they are safe.

He added: “The lesson here is not that cyber criminals only go after big brands. It is that attackers automate this work at huge scale. They scan the internet, test passwords, look for exposed systems and move on to the next target.

“A Derbyshire business with a reused admin password, an exposed VPN login or an out-of-date firewall can be caught in the same dragnet as a multinational.”

The NCSC is advising UK organisations using Fortinet edge devices with SSL VPN enabled to investigate whether they have been affected and monitor networks for unusual activity.

Organisations are being urged to check affected domains using recognised FortiBleed checking tools, confirm whether any listed device belongs to them, review logs for indicators of compromise, and look for signs such as unauthorised account creation or unexpected activity.

Where compromise is suspected, the advice includes isolating the device, preserving logs and configuration evidence, reporting the incident, and considering support from an assured cyber incident response provider.

Kevin said changing passwords alone may not be enough if attackers have already gained a foothold.

He said: “One of the most important parts of the NCSC advice is that simply changing the password may not be sufficient if persistence has been created on the device.

“That sounds technical, but the plain English version is this: if someone has already got inside, they may have left themselves another way back in. You need to check the device properly, not just tidy up the obvious problem.”

Black Swan Cyber Security Solutions is advising local organisations using Fortinet firewalls or VPN services to take the following steps:

- Check whether any Fortinet device or domain appears in the FortiBleed checking tools. https://socradar.io/free-tools/fortibleed or https://www.hudsonrock.com/fortinet
- Confirm whether the device is still in use and belongs to the organisation.
- Review firewall and VPN logs for unusual activity.
- Check for unexpected administrator accounts.
- Remove exposed management interfaces from the internet.
- Update supported devices to the latest version.
- Remove out-of-support systems.

- Change default, generic or reused administrator passwords.
- Enforce multi-factor authentication on VPN and management logins.
- Investigate any other systems that shared the same credentials.

Kevin said: “This is not a time for panic, but it is a time for action. If you use Fortinet, ask your IT provider today whether you are affected, whether SSL VPN is enabled, whether management access is exposed to the internet and whether MFA is enforced.

“For many small organisations, this will be a five-minute question that gives useful reassurance. For others, it may uncover something that needs urgent work.”

Black Swan Cyber Security Solutions works with small businesses, schools, care providers, charities and local organisations across Derbyshire and the surrounding areas, helping them reduce cyber risk in a practical and proportionate way.

Kevin added: “Cyber security does not need to be frightening, expensive or enterprise-level. It needs to be practical, proportionate and clear. This warning is a good reminder that the basics still matter: strong unique passwords, MFA, supported systems, patching, monitoring and knowing what is exposed to the internet.”