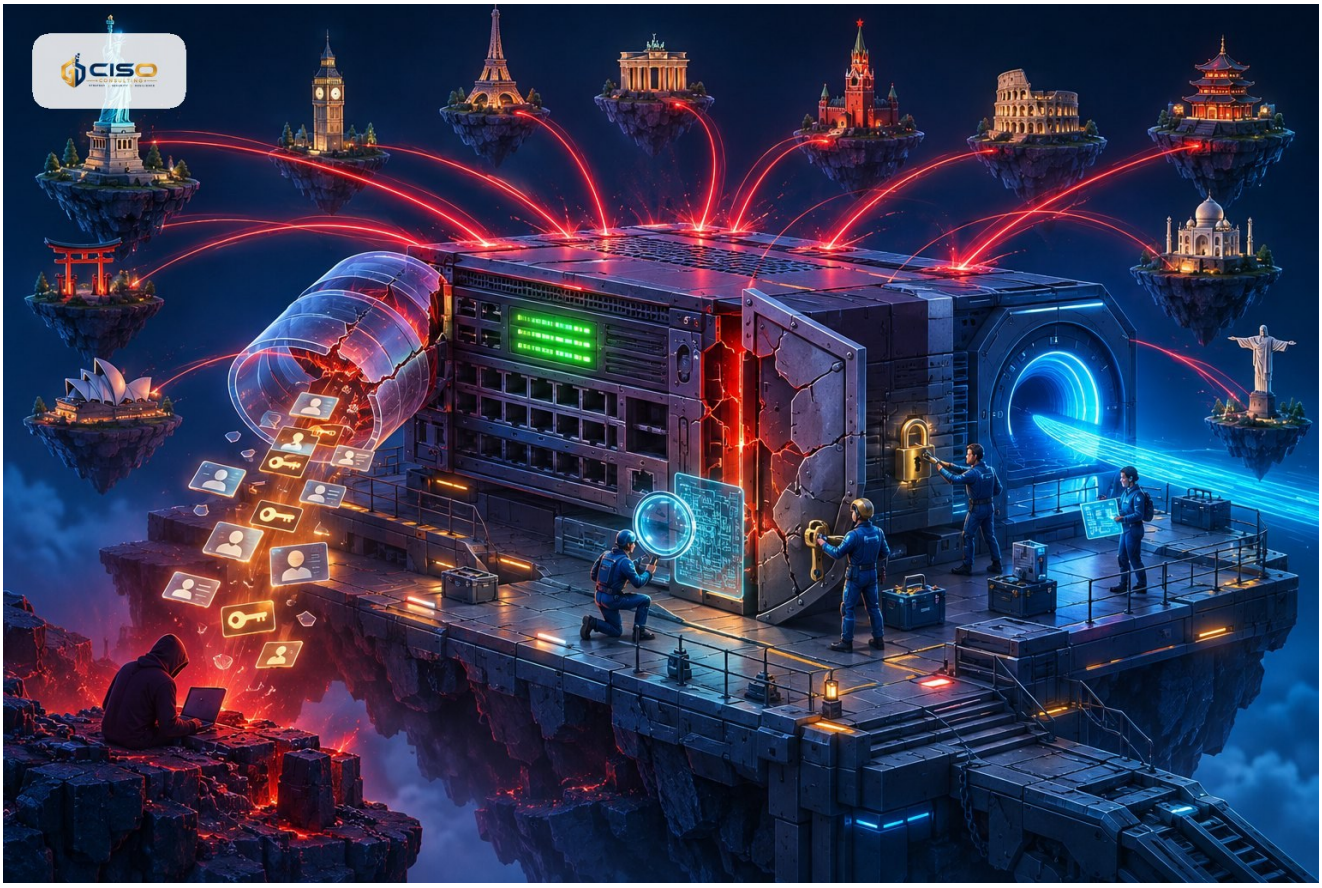
NCSC advises action after global campaign against Fortinet firewalls and VPN gateways



The UK NCSC says Fortinet firewalls and VPN gateways are being targeted globally, and a threat actor has leaked a database of credentials. Organisations should check exposure, look for compromise and harden devices.

- Internet-facing FortiGate and VPN portals were targeted with brute-force, dictionary and credential stuffing attempts.
- A threat actor has leaked a database of credentials; the NCSC notes some indications of potential impact in the UK.
- Two FortiBleed asset checkers, from SOCRadar and Hudson Rock, can be used to check domains.
- If compromise is found, isolate the device and factory reset it, since changing credentials alone may not remove persistence.

> - Hardening includes MFA on all VPN and management logins, no internet-exposed management interfaces, and updated software.

The UK National Cyber Security Centre (NCSC) has issued an alert on a global campaign against Fortinet firewalls and VPN gateways, with some indications of potential impact in the UK. Although the guidance is addressed to UK organisations, the technical advice applies to any organisation running these devices.

What happened

A threat actor has leaked a database of credentials gathered through brute-force, dictionary and **credential stuffing** attempts against internet-facing FortiGate and VPN portals. Credential stuffing relies on passwords stolen from one service being reused on others.

What the NCSC recommends

Organisations with Fortinet edge devices, particularly with SSL VPN enabled, should investigate for malicious activity and monitor the network for unusual behaviour. Priority steps are:

- Check domains with the SOCRadar or Hudson Rock FortiBleed checkers and confirm the device is yours.
- Look for indicators of compromise, including unauthorised account creation and unexpected log activity.
- If compromise is found, isolate the device from the internet and the internal network.
- Preserve logs, configurations and other artefacts, then factory reset the device, as changing credentials alone may not be enough.
- Investigate other edge devices sharing credentials and devices reachable from the affected one.

When re-commissioning, the NCSC advises keeping management interfaces off the internet, updating to the latest version, removing out-of-support systems, replacing default or reused admin passwords, enforcing multi-factor authentication on VPN and management logins, and enabling PBKDF2 for admin accounts.

Fortinet has also published a blog post with guidance and analysis.

What to do now

1. Inventory all Fortinet firewalls and VPN gateways and confirm which ones are internet-facing with SSL VPN enabled.
2. Run your domains through the SOCRadar and Hudson Rock FortiBleed checkers and review Fortinet's published guidance.
3. Review device logs and accounts for indicators of compromise, such as unauthorised admin accounts.
4. For any compromised device, preserve evidence, isolate it, factory reset it, and check devices that share its credentials or are reachable from it.

5. Enforce MFA on all VPN and management logins, remove internet exposure of management interfaces, replace default or reused admin passwords, and update firmware.
6. Report confirmed incidents to the NCA and your sector regulator in line with applicable requirements.