An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC Advisory

Global Targeting of Fortinet Firewalls and VPN Gateways

18th, June 2026

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use **TLP-CLEAR**

when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, **TLP-CLEAR** information may be shared without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

The NCSC is aware of large scale targeting of Fortinet firewall and VPN infrastructure dubbed "**Fortibleed**"[1]. We believe that threat actors have attempted to use previously exposed credentials, brute-force attacks, dictionary attacks, credential stuffing, and exploitation of known vulnerabilities in order to compromise these devices. There has been leaked credentials associated with approximately 74,000 Fortinet devices globally.

Organisations using Fortinet FortiGate firewalls, FortiOS, FortiProxy, SSL-VPN, or internet-facing Fortinet management services should urgently review their exposure, authentication controls and patch status.

Products affected

- Fortinet FortiGate firewalls
- FortiOS
- FortiProxy
- Fortinet SSL-VPN
- Fortinet VPN portals
- Fortinet management interfaces
- FortiManager or FortiAnalyzer where exposed or integrated with affected environments
- Any Fortinet edge device using local, LDAP, RADIUS, SAML, or FortiCloud authentication

Note: The exact affected versions depend on the vulnerability or attack path involved. Organisations should check Fortinet PSIRT advisories and confirm whether deployed firmware is still supported.

Impact

A successful compromise may allow an attacker to:

- Access internal networks remotely
- Bypass perimeter controls
- Steal configuration files and secrets

[1] https://www.hudsonrock.com/blog/fortibleed-75000-fortinet-firewalls-compromised-global-enterprises-exposed-claim-your-ethical-disclosure

- Obtain VPN, LDAP, RADIUS, SAML, local administrator, or pre-shared key credentials
- Modify firewall policies or routing
- Create or alter administrator accounts
- Disable logging or security controls
- Establish long-term persistence
- Conduct lateral movement
- Deploy malware or ransomware
- Exfiltrate sensitive data

Recommedations

- Check the Hudson Rock Fortibleed database for domains related to your organisation: https://www.hudsonrock.com/fortinet
- Rotate Credentials
- Terminate all active SSL VPN and administrative sessions. Reset all Fortinet VPN and administrative passwords, especially on internet-facing systems, and enforce strong password policies.
- Ensure the FortiOs managment console is not exposed to the internet
- Check logs for suspicious behavior. Potential indicators include:
    - Unknown administrator accounts
    - Unexpected VPN users or groups
    - Unexplained configuration changes
    - Log gaps or disabled logging
    - Unexpected firmware changes
    - VPN connections from unfamiliar locations
    - Internal systems accessed by VPN accounts without business justification
    - New firewall rules allowing broader access
    - Unknown certificates or pre-shared keys
    - Unusual outbound connections from the firewall appliance
    - Evidence of downloaded configuration files
- Enforce Multi-Factor Authentication

- Patch devices with the most recent updates from Fortinet
- Monitor the Fortinet PSIRT site for further updates and guidance: https://www.fortiguard.com/psirt

References

- Fortinet: https://www.fortiguard.com/psirt
- Soc Radar: https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised/
- Hudson Rock: https://www.hudsonrock.com/blog/fortibleed-75000-fortinet-firewalls-compromised-global-enterprises-exposed-claim-your-ethical-disclosure
- Double Pulsar: https://doublepulsar.com/fortibleed-75k-fortinet-firewalls-have-admin-passwords-cracked-60299faa65f8
- NCSC UK: https://www.ncsc.gov.uk/news/advice-following-global-targeting-of-fortinet-firewalls-and-vpn-gateways