# FortiBleed: Credential Compromise Campaign Targeting Internet-Facing Fortinet Firewalls and SSL VPN Gateways

June 17th, 2026

| | |
|---|---|
| **Campaign** | FortiBleed: a credential-harvesting operation against Fortinet edge devices. |
| **Attack Type** | Credential stuffing and brute force against exposed Fortinet SSL VPN and admin interfaces, offline cracking of captured SSL VPN authentication hashes, and passive credential collection from compromised devices used as listening posts. Reporting describes lateral movement into internal Active Directory environments. No confirmed Fortinet zero-day and no evidence of a Fortinet product compromise. |
| **Threat Actor** | Unattributed at this time. Reporting points to a Russian-speaking, multi-operator group based on tooling, infrastructure, and victim selection weighted toward NATO member states. Treat attribution as low confidence and developing. |
| **Targeting** | Internet-exposed FortiGate firewalls and SSL VPN gateways across 194 countries and all major sectors. Telecom is the most heavily represented sector by volume. Government entities and critical infrastructure are present. India and the United States account for the largest device footprints. |
| **Impact** | Researchers have confirmed 73,932 unique firewall URLs compromised across 21,632 unique domains. Organizations running exposed Fortinet perimeter devices should treat this as an active threat requiring immediate credential review and access restriction. |

## Executive Summary

A threat actor has assembled and verified a large database of working credentials for internet-facing Fortinet firewalls and SSL VPN gateways. The campaign has been tracked publicly as FortiBleed. SOCRadar published research describing the operation after locating the actor's exposed operational server containing the group's automation, tooling, and a database of verified Fortinet credentials. Independent researcher Volodymyr Diachenko and Hudson Rock reported a related and larger dataset, and Kevin Beaumont published analysis of the likely credential-recovery mechanism.

The operation is a self-feeding loop: the actor scans for Fortinet devices, tests a curated list of credentials leaked in earlier Fortinet incidents, logs every success, and uses compromised devices as

listening posts to harvest more credentials. Much of the recovery stems from legacy hash storage, as devices not re-logged-in after Fortinet's early-2025 PBKDF2 change still store credentials in an older salted SHA-256 format exposed to offline cracking; Diachenko reports the actor cracked captured SSL VPN hashes on a 45-GPU Hashtopolis cluster and moved into internal Active Directory. SOCRadar found no evidence of a Fortinet breach or zero-day and assesses this as credential compromise rather than a product compromise, with generic admin and built-in Fortinet system accounts dominating the dataset.

## Impact

Exposed Fortinet VPN and administrative credentials can enable unauthorized access to internet-facing FortiGate appliances, SSL VPN portals, firewall management interfaces, and downstream internal environments. If valid, these credentials could support account takeover, VPN access, firewall configuration changes, lateral movement, Active Directory compromise, data theft, ransomware staging, and persistence through modified appliance settings. The risk is especially high for organizations exposing FortiGate management interfaces directly to the internet or relying on password-only authentication without MFA.

## Safeguards/Recommendations

- **Check organizational exposure using Hudson Rock's free FortiBleed lookup tool:** Verify whether your domains or Fortinet devices appear in the recovered dataset. ***SRA evaluated organizational exposure against the tool for XDR and Enterprise clients.***
- **Remove Internet Exposure:** Verify FortiOS management interfaces are not exposed to the public internet unless necessary.
- **Eliminate Default Credentials:** Rename or disable built-in and default Fortinet accounts
- **Enforce Strict MFA:** Apply Multi-Factor Authentication to all external gateways and admin interfaces.
- **Practice good Authentication Hygiene**: Enforce unique strong passwords on all admin and SSL VPN accounts, and rotate every credential following any known or suspected compromise, including downstream credentials that may have transited the affected device.
- **Hunt for Anomalous Access**: Review SSL VPN and admin authentication for successful logins from hosting, VPS, or residential-proxy ranges that do not match the user's normal source geography or ISP, particularly for built-in or generic admin accounts, and for configuration export or backup activity originating from unexpected source IPs.
- **Force Credential Rotation & Upgrade Hashing:** Upgrade to the latest FortiOS release and have all admins log back in to force the system to re-hash passwords using the more secure PBKDF2 standard.
- **Assume Compromise:** If you observe any suspected successful logins to admin accounts, assume the device is compromised.
- **Monitor for Stolen Credentials:** Proactively monitor employee and third-party vendor credentials against threat intelligence databases to catch compromised passwords before they are weaponized against your perimeter.

## References


- FortiBleed — 75k Fortinet firewalls have admin passwords cracked
- Fortinet FortiGate Bruteforce Campaign Exposed | Volodymyr "Bob" Diachenko posted on the topic | LinkedIn
- Attackers Exploit Three Fortinet FortiSandbox Flaws, One Patched Last Week
- FortiBleed: 75,000 Fortinet Firewalls Compromised: Global Enterprises Exposed – Claim Your Ethical Disclosure | InfoStealers
- FortiBleed leak exposes Fortinet VPN credentials for 73,000 devices.
- FortiBleed: The Compromise of 30,000 Fortinet Firewalls