FortiBleed Incident Response Checklist

ITKnowledgeBases.com
June 17, 2026

Important: *FortiBleed is not a CVE and is not a confirmed Fortinet zero-day. It is a reported large-scale credential exposure and validation campaign. Several Fortinet CVEs exist in the same period and should be patched separately — they are not the confirmed root cause. Patch status and exploitation details should be verified against current Fortinet PSIRT guidance.*

CLI disclaimer: *FortiOS commands in this checklist are reference examples based on publicly documented syntax. They have not been independently tested by ITKB. Behavior may vary by FortiOS version, device model, and configuration. Validate against Fortinet documentation for your specific version. Test in a non-production or lab environment first where possible. If you are not confident in CLI access on a production firewall, engage a qualified Fortinet engineer or Fortinet support.*

PHASE 1 — Initial Exposure Check

- ☐ **Check Hudson Rock FortiBleed domain lookup**
  hudsonrock.com — a match is an urgent IR trigger; a clean result does not confirm safety
- ☐ **Inventory all internet-facing Fortinet services**
  FortiGate SSL VPN, admin interfaces, FortiManager, FortiAnalyzer, FortiClient EMS, FortiSandbox, FortiProxy, FortiWeb
- ☐ **Determine whether management interfaces are publicly accessible**
  Any public admin interface is a direct risk factor regardless of lookup result

PHASE 2 — Administrator Account Audit

- ☐ **Run: get system admin**
  CLI — validate against your FortiOS version docs before running in production
- ☐ **Identify unknown local admin accounts**
  Accounts not tied to a known person or approved service
- ☐ **Flag generic account names**
  e.g. secadmin, backup, svc_admin, or similar
- ☐ **Check account creation timestamps against change log**
  Accounts created outside a documented change window are a red flag
- ☐ **Review account privilege levels**
  Accounts with higher privilege than expected should be investigated
- ☐ **Check for stale accounts from former staff or vendors**
  Remove or disable anything that cannot be validated

PHASE 3 — SSL VPN Session Review

- ☐ **Run: get vpn ssl monitor**
  CLI — validate against your FortiOS version docs before running in production
- ☐ **Run: diagnose vpn ssl list**
  CLI — validate against your FortiOS version docs before running in production
- ☐ **Flag logins from unexpected countries**
  Countries where your users do not operate

- [ ] **Flag logins from VPS or hosting provider ASNs**
  Legitimate logins rarely originate from cloud hosting infrastructure
- [ ] **Check for impossible travel**
  Same account, geographically distant logins within a short time window
- [ ] Check for multiple concurrent sessions per user
- [ ] Review access timestamps relative to user time zones
- [ ] Flag successful logins immediately following repeated failures
- [ ] **Correlate VPN logs with SIEM and identity provider sign-in logs**
  VPN data alone may not provide full context

PHASE 4 — Admin Login & Configuration Event Review

- [ ] Review Log & Report > System Events in FortiOS GUI
- [ ] **Flag successful admin logins from unexpected source IPs**
  Use ITKB IP Geolocation to review country, ISP, and ASN context
- [ ] Check for new administrator account creation events
- [ ] Check for privilege changes on existing accounts
- [ ] **Check for configuration download or export events**
  Any export not correlated to an approved change should be escalated
- [ ] Check for changes to VPN users or groups
- [ ] Check for changes to trusted host restrictions
- [ ] Check for changes to MFA or two-factor authentication settings
- [ ] **Check for disabled or reduced logging**
  Attackers may reduce logging to hide activity

PHASE 5 — Persistence Indicator Hunt

- [ ] Verify no unauthorized local admin accounts remain
- [ ] Verify no unauthorized VPN user accounts exist
- [ ] Review firewall policies for unexpected changes
- [ ] Check for new automation stitches or scripts
- [ ] Check for unexpected scheduled tasks or recurring jobs
- [ ] Review for unfamiliar API integrations or admin sessions
- [ ] Check for new or unexpected trusted host entries
- [ ] Check for changes to logging destinations
- [ ] Check for unexpected certificate changes or new SAML/SSO configurations

PHASE 6 — Source IP Investigation

- [ ] Collect: source IP, country, ASN, ISP, hostname, timestamp, username, action, success/fail
- [ ] **Run suspicious IPs through ITKB IP Geolocation Tool**
  itknowledgebases.com/ip-geolocation — free, no account required
- [ ] Flag IPs from countries with no operational presence
- [ ] **Flag IPs resolving to hosting/VPS provider ASNs**
  e.g. DigitalOcean, Vultr, Hetzner, Linode
- [ ] Flag known anonymization services or Tor exit nodes
- [ ] Flag rotating or distributed IP ranges with repeated attempts
- [ ] Flag successful logins from networks with no prior activity

PHASE 7 — Immediate Remediation

- [ ] Rotate all FortiGate administrator passwords
- [ ] Rotate all SSL VPN user passwords
- [ ] Rotate local firewall service accounts, shared/vendor accounts, break-glass accounts
- [ ] Rotate API keys or tokens where applicable
- [ ] Rotate credentials reused on other systems
- [ ] **Enforce MFA on SSL VPN and admin access**
  Prefer FIDO2 or certificate-based; TOTP is better than none
- [ ] **Restrict FortiGate management interface from public internet**
  Internal networks, VPN-only, or approved source IPs only
- [ ] Terminate suspicious active VPN sessions
- [ ] Disable or remove unknown admin and VPN user accounts
- [ ] **Preserve logs before they roll over**
  FortiGate events, SSL VPN, admin logins, config changes, IDP, SIEM, EDR, AD/Entra ID

PHASE 8 — Patching (Separate from FortiBleed Root Cause)

- [ ] **Verify FortiOS patch status per Fortinet PSIRT**
  fortiguard.fortinet.com/psirt
- [ ] **CVE-2026-35616 — FortiClient EMS 7.4.5–7.4.6 improper access control (CISA KEV)**
  NVD: nvd.nist.gov/vuln/detail/CVE-2026-35616
- [ ] **CVE-2026-21643 — FortiClient EMS 7.4.4 SQL injection**
  NVD: nvd.nist.gov/vuln/detail/CVE-2026-21643
- [ ] **CVE-2026-24858 — FortiCloud SSO auth bypass, multiple products (CISA KEV)**
  NVD: nvd.nist.gov/vuln/detail/CVE-2026-24858

- **CVE-2026-39813 — FortiSandbox JRPC API path traversal, CVSS 9.1**
  Fortinet PSIRT lists Known Exploited: No — verify current advisory
- **CVE-2026-39808 — FortiSandbox OS command injection**
  CVE.org: cve.org/CVERecord?id=CVE-2026-39808
- **CVE-2026-25089 — FortiSandbox/Cloud/PaaS OS command injection**
  NVD: nvd.nist.gov/vuln/detail/CVE-2026-25089
- Verify FortiClient EMS, FortiManager, FortiAnalyzer, FortiProxy, FortiWeb patch status

PHASE 9 — If Unauthorized Admin Access Is Confirmed

- Preserve current logs and device configuration before making changes
- Document all indicators of compromise
- Compare current config to a known-good baseline
- Identify and document all unauthorized configuration changes
- Rotate all related credentials
- Validate firmware integrity and patch level
- Consider factory reset and rebuild from verified baseline if config integrity is in doubt
- Escalate to incident response

ITKB TOOLS FOR FORTIBLEED TRIAGE

IP Geolocation Tool
itknowledgebases.com/ip-geolocation/
Geolocate suspicious VPN and admin login source IPs. Returns country, ISP, and ASN. Free, no account required.

DNS Lookup Tool
itknowledgebases.com/dns-lookup/
Investigate suspicious domains and hostnames encountered during log review.

Safe Link Decoder
itknowledgebases.com/safe-link-decoder/
Decode Microsoft Safe Links and wrapped URLs during phishing and credential-theft investigations.

Security Advisories
itknowledgebases.com/advisory/
Current vulnerability advisories and remediation notes for IT and SOC teams.

Sources

Hudson Rock — FortiBleed analysis and lookup — hudsonrock.com/blog/fortibleed-75000-fortinet-firewalls-compromised-global-enterprises-exposed-claim-your-ethical-disclosure
SecurityWeek — SOCRadar and FortiSandbox reporting — securityweek.com/3-recently-patched-fortinet-fortisandbox-vulnerabilities-in-hacker-crosshairs/
Fortinet PSIRT FG-IR-26-112 — CVE-2026-39813 — fortiguard.fortinet.com/psirt/FG-IR-26-112
NVD — CVE-2026-35616 — nvd.nist.gov/vuln/detail/CVE-2026-35616
NVD — CVE-2026-21643 — nvd.nist.gov/vuln/detail/CVE-2026-21643
NVD — CVE-2026-24858 — nvd.nist.gov/vuln/detail/CVE-2026-24858
NVD — CVE-2026-25089 — nvd.nist.gov/vuln/detail/CVE-2026-25089

CVE.org — CVE-2026-39808 — cve.org/CVERecord?id=CVE-2026-39808