EOTISEC
ANALYTICAL INTELLIGENCE REPORT

EOTISEC Analytical Division

Report Title	**FortiBleed: Mass Credential Compromise of Internet-Facing Fortinet FortiGate Firewalls and SSL VPN Gateways**
Report Number	**EOTISEC-2026-045**
Supersedes	**EOTISEC-2026-044 (18 June 2026)**
Date of Report	**23 June 2026**
Coverage Period	**December 2025 — June 23, 2026**
Classification	**SENSITIVE BUSINESS DOCUMENT**
Originator	**EOTISEC Analytical Division**
Subject	**A criminal initial access broker has assembled a validated, searchable database of working administrator and SSL VPN credentials for internet-exposed Fortinet FortiGate devices across 194 countries. The campaign is active and the dataset is now being sold. Fortinet has confirmed the activity is credential reuse plus brute force rather than a new vulnerability. Post-exploitation tooling overlaps with state-sponsored tradecraft, indicating the credential pool is reaching more capable actors.**
Customer Sector	**Information Technology and Communications (DHS Critical Infrastructure Sector). Secondary: Financial Services, Government Facilities, Energy, Defense Industrial Base**
Distribution	**Subscribers**

SECTION 1: SCOPE AND PURPOSE

This report is a point update to EOTISEC-2026-044 (18 June 2026) and supersedes it. It assesses the credential compromise campaign tracked publicly as FortiBleed, disclosed in mid June 2026 and affecting internet-facing Fortinet FortiGate firewalls and SSL VPN gateways. The assessment is written for subscribers who operate, defend, or carry counterparty exposure to Fortinet perimeter devices. It draws on the original discovery by independent researcher Volodymyr Diachenko, corroborating analysis by Kevin Beaumont in collaboration with Hudson Rock, an independent infrastructure discovery by SOCRadar, the Fortinet PSIRT statement of 19 June, CISA and UK NCSC advisories, and reporting by Bitsight, Palo Alto Unit 42, Huntress, SpyCloud, IBM X-Force, BleepingComputer, Help Net Security, CSO Online, Security Affairs, and Arctic Wolf. The report draws exclusively from open source reporting, government data releases, and market data.

Material developments since the 18 June version drive this update. Fortinet published a formal incident statement on 19 June. CISA issued a hardening alert on 18 June and updated it on 22 June, and the UK NCSC issued a parallel warning. SOCRadar consolidated its device count and published deeper analysis of the operators' tooling and a dated account of a defense-sector exfiltration. The dataset, which had not

yet been offered for sale at the time of the prior report, is now being sold on a criminal forum, and security firms have identified post-exploitation tooling that overlaps with state-sponsored tradecraft. These developments resolve two of the four intelligence gaps from the prior version and shift two confidence levels, as noted in Sections 2 and 4.

Confidence in this product is uneven by design, and the reader should treat the judgments below as carrying different evidentiary weight. The fact that a large, validated credential set exists and that the operation remains active rests on direct verification by multiple independent parties and is assessed with high confidence. The precise count of affected devices rests on figures that the disclosing parties themselves describe as not independently verifiable, and is assessed with moderate confidence. The method by which device configurations were first obtained rests on circumstantial indicators and competing expert readings, and is assessed with low confidence. The core operators are now better characterized as a criminal initial access broker, assessed with moderate confidence. No element of this report attributes the FortiBleed campaign itself to a nation-state, because no source does so as of the issue date.

SECTION 2: KEY JUDGMENTS

Judgment 1: Validated Credential Set and Active Campaign — CONFIRMED

We assess with **high confidence** that a threat actor has assembled a validated, searchable database of working administrator and SSL VPN credentials for internet-exposed Fortinet FortiGate devices, and that the operation was still running at the time of disclosure. Independent verification of a sample of live, working logins by a recognized researcher, combined with a separately discovered operational server holding the operators' tooling and victim database, supports this judgment.[1][2]

Judgment 2: Scale of the Compromise — CONSOLIDATED

We assess with **moderate confidence** that the validated credential set covers roughly 86,644 distinct devices, the figure SOCRadar consolidated on after its full investigation, representing approximately half of the internet-facing Fortinet population. SOCRadar initially reported over 30,000 and revised upward to 86,644 confirmed working credentials as the analysis progressed. The firmest floor remains the roughly 30,791 credentials independently validated as working, and counts still vary by what each party measures, so the upper figure should be read as the disclosing party's own consolidated number rather than an independently confirmed total.[1][2][3][4]

Judgment 3: Initial Access Vector — UNRESOLVED

We assess with **low confidence** that the configuration files underpinning the credential set were obtained through a combination of known unpatched authentication-bypass vulnerabilities, recycled credentials from prior leaks and infostealer logs, and possibly an undisclosed access method. Expert readings diverge, and the access vector has not been established by any party.[3][5][6]

Judgment 4: Attribution — CRIMINAL INITIAL ACCESS BROKER, RUSSIAN-SPEAKING

We assess with **moderate confidence** that the core operators are a financially motivated, Russian-speaking criminal initial access broker, based on tooling with Cyrillic-language comments, a victim set weighted toward NATO member states, and the dataset's initial-access-broker formatting. This is firmer than the prior version: an initial access broker on the Russian-language forum Exploit.in claimed responsibility on 16 June and offered the credentials for sale, a claim Unit 42 noted it had not validated, and SpyCloud assessed the operation began on 19 May as a live initial-access-broker campaign. Fortinet's

own statement of 19 June characterizes the activity as credential reuse from prior incidents plus brute force against devices with weak password hygiene and no MFA. Large-scale brute-force and credential-access campaigns against perimeter and cloud services by Russian-speaking operators are an established pattern, documented in the 2021 joint NSA, CISA, FBI, and NCSC advisory on a global brute-force campaign, which lends the attribution surface plausibility without identifying this specific group.[23] The criminal core and the state nexus are addressed separately in Judgment 6.[1][7][25][30]

Judgment 5: Lateral Movement Risk — NOW MATERIALIZING

We judge it **likely** that the most consequential near-term risk to affected subscribers is the use of the credential set as a foothold for lateral movement into internal networks, including Active Directory environments. This is no longer only forward-looking. Reporting indicates buyers have used purchased credentials to pivot into Active Directory, deploy tunneling tools, and stage ransomware, and the exposed data includes Kerberos hashes rather than VPN credentials alone, which widens the exposure from the perimeter device to internal identity systems.[5][8][24][29][31] The risk is highest for organizations that operate flat networks, reuse administrator credentials across perimeter and internal systems, or have not segmented management access.

Judgment 6: State-Actor Nexus — TOOLING OVERLAP, NOT CAMPAIGN ATTRIBUTION

We assess with **moderate confidence** that the FortiBleed credential pool is reaching actors more capable than the criminal broker that assembled it, and we judge it **likely** that some of that downstream use is state-aligned, based on post-exploitation tooling that overlaps with documented state tradecraft. We state the limit plainly: no source attributes the FortiBleed campaign itself to a nation-state, and this judgment concerns downstream use, not origin. Bitsight identified the tunneling tools Chisel and Neo-reGeorg in the related post-exploitation activity, both previously seen in state-sponsored campaigns against Fortinet perimeter devices, and assessed the credential pool is being used for both opportunistic criminal access and targeted intrusion. This sits against a documented history in which China-linked Volt Typhoon and Salt Typhoon have used Fortinet edge devices as an initial-access vector for espionage against critical infrastructure and telecommunications. The espionage dimension treated as a low-confidence possibility in the prior version is now supported at the tooling level, though it falls short of named attribution.[29][32][33][34]

SECTION 3: SITUATION AND BACKGROUND

Fortinet FortiGate firewalls and SSL VPN gateways are among the most widely deployed network perimeter devices in the world, controlling access to internal networks across virtually every sector. A compromised FortiGate is therefore not a single-host problem. The device sits at the boundary of the protected network, holds credentials and routing configuration, and can be reconfigured by an administrator-level account to grant further access. This combination of ubiquity and privilege is the reason Fortinet perimeter devices have been a recurring target of both criminal and state-aligned operators over the past several years.

The FortiBleed dataset surfaced in mid June 2026. Independent researcher Volodymyr Diachenko reported finding an internet-exposed server holding what appeared to be valid Fortinet VPN credentials, including usernames, email addresses, and plaintext passwords, for organizations worldwide.[6] Kevin Beaumont independently reviewed portions of the data, obtained the wider set through Hudson Rock, and confirmed that a sample of the administrator logins and passwords were authentic and that affected devices remained online and reachable.[3][5] Separately, SOCRadar reported discovering the operators' own infrastructure, including automation scripts, credential-testing tooling, logs, and a victim database organized by country, sector, and revenue.[1]

Why the Name Overstates the Mechanism

The label FortiBleed evokes Heartbleed and implies a single dramatic memory-disclosure flaw in the product. The evidence does not support that framing. SOCRadar stated plainly that it found no evidence Fortinet itself had been compromised or that a zero-day was involved, and assessed the credentials were most likely obtained through brute-force and credential-stuffing against internet-facing services.[1] Fortinet has since put its position on record. In a PSIRT blog published 19 June by Carl Windsor, the company stated that the activity involves threat actors reusing credentials from previous incidents, referenced internally as FG-IR-26-060 and FG-IR-25-647, and employing brute-force techniques against devices with weak password hygiene and no multi-factor authentication, and that this is not a new Fortinet vulnerability and is not related to any recent incident or advisory.[25] The naming is doing rhetorical work that the confirmed facts do not. The vendor framing is technically defensible, though the security community contests it on the ground that the failure to automatically re-hash credentials on firmware upgrade looks more like a design defect than administrator error. We retain the name FortiBleed only because it is the common public identifier, not because it describes a discrete vulnerability.

LINCHPIN ASSUMPTION

This assessment assumes the credential set is what the disclosing parties represent it to be: a collection of working credentials harvested from device configurations, rather than a recycled aggregation of older leaks repackaged to appear new. ***If that assumption is wrong*** *and the bulk of the data is stale, as Fortinet's framing partly suggests and as occurred with the 2025 Belsen Group leak, the near-term risk to organizations that have rotated credentials since their last known exposure falls sharply, and the analytic line shifts from active compromise toward residual exposure. The independent verification of live, working logins by Beaumont is the single most important piece of evidence holding this assumption in place. If that verification were shown to rest on a small or unrepresentative sample, confidence in the scale judgment would degrade in step.[3][4][9]*

SECTION 4: ANALYSIS

The campaign combines three technical elements: extraction of device configuration files, offline cracking of credential hashes contained in those configurations, and a self-reinforcing harvesting loop that recycles recovered credentials back into the operation. Each is discussed below. The reader should note that the first element, how configurations were obtained, is the least understood and the point on which expert opinion diverges most sharply.

4.1 Evidence of Configuration-Level Exfiltration

The strongest technical signal in the dataset is that it contains information available only from inside a device configuration export, not from a login screen. Beaumont noted that the data includes internal email addresses and other elements visible only on the device itself, and stated that the data appears to have come from exports of configuration from the devices.[5][3] This distinguishes FortiBleed from a simple credential-scrape against a login interface and points to configuration-level access. One technical account describes the decryption path in concrete terms: FortiGate configuration files are encrypted, but the encryption key is derived from the device serial number, which is often visible on the management interface login page, so possession of the configuration file and the serial number makes decryption straightforward.[9]

4.2 The Hashing Weakness That Made Cracking Feasible

Older FortiOS versions stored administrator credentials using a legacy SHA-256 with salt scheme. SHA-256 is a fast hash, which is desirable for integrity checking and damaging for password storage, because speed is exactly what an offline cracker exploits.[3] Fortinet hardened credential storage in early 2025 by

migrating to PBKDF2 with a randomized salt, a deliberately slow scheme that resists offline cracking. Arctic Wolf documented the precise versions: PBKDF2-based hashing was introduced in FortiOS 7.2.11, 7.4.8, and 7.6.1, replacing the legacy SHA-256 storage.[10]

The protection had a critical gap. When a device was upgraded from an earlier version, existing administrator passwords remained stored as SHA-256 hashes until the corresponding administrator logged in again after the upgrade.[10] Many devices were upgraded but never had every administrator log back in, so they continued to store crackable SHA-256 hashes. Arctic Wolf further noted, citing Fortinet, that even after a password is updated to PBKDF2 the previous SHA-256 hash is retained in a hidden old-password setting for backward compatibility, which has its own residual-exposure implications.[10] Beaumont's analysis attributes the cracking to a distributed cluster, reported variously as 45 or 48 GPUs, managed through the open-source Hashtopolis framework, capable of pushing very large candidate volumes per second against fast hashes.[3][11]

Note on a Numeric Discrepancy

Public reporting cites the cracking cluster as both 45 GPUs and 48 GPUs across otherwise reliable outlets. The discrepancy is immaterial to the assessment, since either figure supports the same conclusion about offline cracking capability, but it is flagged here so the reader does not treat a single precise figure as settled.[3][11]

4.3 The Self-Reinforcing Harvesting Loop

SOCRadar's reconstruction from the operators' own infrastructure describes a fully automated cycle. The operators scan the internet for Fortinet devices, test each against a curated list of known passwords, and record every successful login. A compromised device is then used as a listening post to capture additional credentials passing through it, and those credentials are fed back into the scanner to compromise further devices, so the system feeds itself.[1] The password list is not random. It is assembled from credentials leaked in earlier Fortinet incidents, which works precisely because many organizations never rotated credentials after a prior breach.[1] Diachenko's reconstruction describes the operators intercepting SSL VPN authentication hashes, cracking them offline, and using the recovered passwords to pivot into internal Active Directory environments.[6][8]

SOCRadar's deeper analysis named the tooling that drives the loop. The core collector is FortigateSniffer, also tracked as fg_sniffer, a Golang tool compiled for both Linux and Windows that turns a compromised firewall into a password collector. SOCRadar traced the campaign to 260 operational servers, dated it as running since at least February 2026, and counted 659 discrete harvest cycles, with infrastructure still partially active at the time of its analysis.[1][28] This named, multi-server tooling upgrades the earlier generic description of automation scripts to an attributable toolset.

4.4 Scale Figures and Why They Disagree

The reported scale varies by source, and the variation is itself analytically important. The table below records the principal figures as stated by each party, without reconciling them into a single number, because the disclosing parties have not reconciled them and have stated the totals cannot be independently verified.[2][3][4]

Source	Reported Figure	Basis as Stated
Hudson Rock / Beaumont	**73,932 URLs; ~75,000 devices**	Approx. 50% of internet-facing Fortinet firewalls indexed by Shodan at disclosure

Source	Reported Figure	Basis as Stated
SOCRadar	86,644 devices; 80,000+ IPs	Count of entries in the operators' own validated database
SOCRadar (verified)	30,791 working credentials	Subset SOCRadar independently validated as working
Arctic Wolf	30,000 to 75,000 devices	Range across the analyses it reviewed
Diachenko (attempts)	~1.16 billion attempts	Against 320,777 FortiGate targets, plus 2.1 billion against 163,650 MSSQL servers, per recovered logs

Two observations follow. First, the verified subset of roughly 30,791 working credentials is a firmer floor than the headline 73,000 to 87,000 device counts, and a cautious reader should anchor on the verified floor rather than the upper estimates.[1][2] Second, the campaign reached well beyond Fortinet: the same operators ran a parallel brute-force effort against more than 160,000 Microsoft SQL Server systems, which indicates a broad credential-access operation rather than a Fortinet-specific exploit.[6]

4.5 MITRE ATT&CK Mapping

The observed and reported behaviors map to the following ATT&CK techniques. The mapping reflects activity described by the disclosing parties. Techniques tied to the unconfirmed initial access vector are marked as assessed rather than confirmed.

Technique	Name	Tactic	Basis
T1595	Active Scanning	Recon	Confirmed
T1190	Exploit Public-Facing Application	Initial Access	Assessed
T1133	External Remote Services	Initial Access	Confirmed
T1110.002	Brute Force: Password Cracking	Credential Access	Confirmed
T1557	Adversary-in-the-Middle	Collection	Reported
T1003	OS Credential Dumping (config extraction)	Credential Access	Assessed
T1078	Valid Accounts	Initial Access	Confirmed
T1136	Create Account (backdoor admin)	Persistence	Reported
T1556	Modify Authentication Process	Defense Evasion	Assessed

On the defensive side, the relevant MITRE D3FEND countermeasures are credential rotation and revocation, multi-factor authentication enforcement, network traffic filtering to remove management-interface exposure, and inbound session analysis to detect anomalous administrative logins. These are reflected in the recommendations in Section 5.

4.6 The Initial Access Question

The unresolved question at the center of this campaign is how the operators first obtained device configurations at scale. The disclosing parties agree they do not know. BleepingComputer reported that none of Diachenko, Hudson Rock, or Beaumont had identified how the configuration data was originally obtained, and that it was unclear whether it came from previously disclosed vulnerabilities, a newly

discovered flaw, or another method.[6] CSO Online recorded the same gap, quoting researchers that the initial access vector is presently unknown.[8] We therefore present the competing hypotheses rather than asserting a conclusion.

Hypothesis A: Known Unpatched Vulnerabilities

The leading candidate among disclosed flaws is CVE-2026-24858, a FortiCloud single sign-on authentication bypass. CISA, citing Fortinet, assigns it CWE-288 and a CVSS score of 9.4, and added it to the Known Exploited Vulnerabilities catalog on 27 January 2026 with a federal remediation deadline of 30 January 2026.[12][13] On devices with FortiCloud SSO enabled, an attacker with their own FortiCloud account and a registered device could authenticate to other customers' devices, create local administrator accounts for persistence, and make unauthorized configuration changes, behavior Arctic Wolf observed directly.[12][14] Critically, this flaw compromised devices that were fully patched against the December 2025 SSO bypasses CVE-2025-59718 and CVE-2025-59719, which means patch currency alone did not protect against it.[12][15] This hypothesis fits the observed configuration exfiltration, but it is constrained. FortiCloud SSO is not enabled by default, and the number of exposed SSO-enabled devices was in the low tens of thousands and falling after disclosure, which is smaller than the FortiBleed device count.[15]

Hypothesis B: An Undisclosed Vulnerability

Beaumont raised the possibility that the operators used a previously unknown flaw to obtain configurations, reasoning from the breadth of the data and the presence of devices on recent patches.[3][11] This hypothesis explains why the dataset includes devices that appear current, but it rests on inference from effect rather than on any identified flaw, and no such vulnerability had been confirmed by Fortinet as of the issue date.[3]

Hypothesis C: Recycled Credentials and Infostealer Logs

SOCRadar's position is that the credentials were most likely obtained through brute-force and credential-stuffing using credentials leaked in earlier incidents, with no Fortinet zero-day involved.[1] Fortinet's own statement matches this in part, describing the data as a mix of information from previous incidents and brute-forced credentials.[4] This hypothesis is the most parsimonious and best explains the parallel MSSQL campaign, but it sits in tension with the configuration-level artefacts Beaumont identified, which credential-stuffing alone would not produce.[5]

The most defensible reading, and the one we adopt at low confidence, is convergence rather than a single cause: known unpatched flaws on some devices, an undisclosed method on others, and recycled credentials across the rest, with offline cracking of weak hashes tying the set together. We flag explicitly that this convergence reading is partly a function of incomplete evidence, and that it should not harden into a settled conclusion as further analysis emerges.

4.7 Historical Pattern of Comparable Activity

FortiBleed is not an isolated event but the latest in a multi-year pattern of credential and configuration compromise targeting Fortinet perimeter devices. Placing it against prior incidents both calibrates the scale claims and clarifies what is and is not novel about it.

Belsen Group, January 2025

In January 2025 a threat actor calling itself Belsen Group released full configuration files and VPN credentials for more than 15,000 FortiGate devices, organized by country and IP address, free of charge on a criminal forum.[16][17] Beaumont and CloudSEK assessed the data had been collected in October 2022 through exploitation of the authentication-bypass flaw CVE-2022-40684 while it was a zero-day, with SSL VPN credentials sourced via the older path-traversal flaw CVE-2018-13379.[17][18] Fortinet confirmed

the configurations were genuine but characterized the release as dated 2022 data aggregated to appear new, noting most affected devices had long since been upgraded.[19] Censys found that as of mid-January 2025 over half the 15,469 compromised hosts were still online and roughly a third still exposed their web login interfaces, which is why aged configuration data remained dangerous.[20] Beaumont states the FortiBleed IP addresses are largely different from the Belsen set, indicating a more recent and larger collection rather than a rerelease.[3][5]

The 2021 SSL VPN Credential Dump

In September 2021 a threat actor published SSL VPN credentials for nearly half a million Fortinet accounts, harvested by exploiting the same CVE-2018-13379 path-traversal flaw later implicated in the Belsen leak.[17] That incident established the template that recurs through FortiBleed: a known, patchable flaw, a long tail of unpatched or unrotated devices, and credentials that retain value for years because organizations fail to rotate them after exposure.

The December 2024 Management-Interface Campaign

Arctic Wolf documented a campaign beginning in early December 2024 against FortiGate devices with management interfaces exposed on the public internet. At the time the point of intrusion was not tied to a specific CVE.[19] This episode prefigures the central FortiBleed risk factor, namely management-interface exposure, which Beaumont reports characterizes a majority of the FortiBleed-affected devices.[5]

The FortiCloud SSO Bypass Chain, December 2025 to January 2026

The immediately preceding episode is the FortiCloud SSO bypass chain. CVE-2025-59718 and CVE-2025-59719, disclosed in December 2025, allowed unauthenticated attackers to bypass SSO via crafted SAML messages, and observed attacks involved authenticating as admin and immediately downloading the system configuration file, which contains hashed credentials.[15][21] When patched devices continued to be breached in January 2026, Fortinet identified the net-new CVE-2026-24858, disabled FortiCloud SSO service-wide on 26 January 2026, and issued its advisory on 27 January 2026.[12][13][22] This chain is the strongest historical link to FortiBleed because its documented outcome, attacker-driven download of configuration files containing hashed credentials, is exactly the artefact FortiBleed monetized at scale.[21]

4.8 Impact Assessment

The impact of FortiBleed is best understood not as the value of the credentials themselves but as the access those credentials unlock. Beaumont states the practical effect directly: with a working credential an attacker can log in remotely and gain access to the firewall and therefore the network behind it, change settings including security controls, and create backdoor administrator accounts.[8] A compromised perimeter device is a position from which to move laterally, not an endpoint of the attack.

Sectoral and Geographic Exposure

SOCRadar's analysis of the victim database found exposure across every major sector, with telecommunications the most heavily represented by volume at 5,616 entries, a concern that compounds because telecom infrastructure underpins communications for other sectors.[1] Government exposure totalled 591 entries across 111 domains, with India accounting for over 60% of government entries, and the dataset also reaches banks, hospitals, universities, energy companies, and large multinationals.[1] Geographically, India and the United States together account for nearly a third of all entries, with the remainder spread across Asia, Europe, the Americas, the Middle East, and Africa.[1] Enterprises above one billion dollars in revenue account for over 20% of entries.[1]

The Lateral Movement Risk

The documented pivot from FortiGate credentials into internal Active Directory environments is the mechanism by which a perimeter compromise becomes a domain compromise.[6][8] Where a firewall account is reused for, or trusted by, internal directory services, recovery of the firewall credential can seed privilege escalation inside the network. The risk is highest for organizations that operate flat networks, reuse administrator credentials across perimeter and internal systems, or have not segmented management access.

The Reported Defense-Sector Exposure

The prior version held the defense-sector compromise at low confidence as a single-sourced Diachenko claim. It now has a second, more detailed account. SOCRadar's Threat Research Unit reported that on 15 June, following offline cracking of 172 Kerberos RC4 hashes, the operator executed a targeted exfiltration against a NATO-aligned defense contractor, using a script that recursively extracted full DFS shares over SMB and streamed them directly to attacker SSH servers without local staging, and SOCRadar's CISO described the operation as ending in real exfiltration including from that contractor.[28] Diachenko separately reported that at least four organizations across Japan, Taiwan or Vietnam, Iraq, and Turkey were fully compromised, including a Turkish NATO defense contractor from which classified defense documents were allegedly exfiltrated.[24] On the strength of the dated, technical second account, we raise this from low to moderate confidence, while noting it still rests on the disclosing-research community rather than victim or government confirmation.

The Initial-Access-Broker Indicator

A structural feature of the dataset points to its intended use. Beaumont and others note that each entry carries the organization's industry, revenue, employee count, and country, formatted in the manner common to initial access listings sold in criminal markets.[5][6] The prior version noted the set had not yet appeared for sale and that a closing window existed. That window has closed. Bitsight confirmed at least one threat actor selling FortiBleed-related content on a Russian cybercrime forum, and Unit 42 reported an initial access broker on Exploit.in claiming responsibility and offering the credentials for sale on 16 June.[29][30] Threat actors who were not part of the original campaign are now working through the public, growing dataset opportunistically, and the downstream impact is already countable: Huntress cross-referenced the leaked addresses against its own data and identified 845 partner organizations specifically affected.[27]

4.9 The State-Actor Nexus

Given the subscriber interest in nation-state exposure, this subsection sets out what the sourcing does and does not support. The headline is a boundary: no source attributes the FortiBleed campaign itself to a nation-state. The responsible-party claim points the other way, toward crime. An initial access broker on the Russian-language forum Exploit.in claimed the campaign and offered the data for sale, and SpyCloud dated the operation's start to 19 May as a live initial-access-broker effort.[30] The state dimension enters not at the origin of the campaign but at the downstream use of its output.

The evidence for that downstream state use is tooling overlap. Bitsight identified the tunneling tools Chisel and Neo-reGeorg in the post-exploitation activity tied to the related CVE exploitation, both previously observed in state-sponsored campaigns against Fortinet perimeter devices including Volt Typhoon, and concluded the credential pool is being drawn on for both opportunistic criminal access and targeted intrusion by sophisticated, well-resourced actors.[29] Tooling overlap is suggestive, not dispositive, because criminal and state operators borrow each other's tools, but it is a meaningful signal when the same tools recur in campaigns against the same class of device.

The historical context makes the concern concrete. Fortinet edge devices are a documented favorite initial-access vector for two China-linked groups in particular. Microsoft attributed to Volt Typhoon a years-long

campaign against critical infrastructure on Guam, a key military hub, in which the group directed many intrusions against FortiGate appliances, harvested credentials, and moved laterally using living-off-the-land techniques.[32] Salt Typhoon, China-linked and active since 2019, has exploited Fortinet among other edge vendors in espionage operations against telecommunications and government targets, including a campaign against US telecommunications carriers.[33] A 2026 Congressional Research Service summary identifies China, Russia, Iran, and North Korea as the most active state actors in this space and cites both Typhoon operations as recent critical-infrastructure cases.[34]

The defensible synthesis is a two-tier threat. At the core is a criminal initial access broker that harvested and is selling the credentials. Drawing from the same pool are more capable actors, some of whose tooling overlaps with documented Chinese state tradecraft, against a backdrop in which Fortinet edge devices are a known state initial-access vector and the confirmed exfiltration target was a NATO-aligned defense contractor. For a subscriber assessing nation-state exposure, the operational implication is that appearance in the FortiBleed dataset is not only a criminal-access problem but a potential espionage-access problem, and the response, immediate credential rotation and management-interface withdrawal, is the same for both.

4.10 The Linchpin Assumption and Alternative Readings

The load-bearing assumption is identified in the callout in Section 3 and is not repeated here. The principal alternative reading worth weighing against the active-compromise framing is Fortinet's: that the data is substantially dated and aggregated to appear new, mirroring the vendor's 2025 Belsen characterization. The evidence that holds the active-compromise reading in place is Beaumont's verification of live working logins on currently reachable devices and the largely novel IP set relative to Belsen.[3][5][19] We weigh both, retain the active-compromise reading at the confidence stated in the Key Judgments, and treat the dated-data alternative as the most credible competing hypothesis rather than as refuted.

SECTION 5: DECISION SUPPORT AND RECOMMENDATIONS

The following actions reflect converging guidance from CISA, the UK NCSC, Arctic Wolf, SOCRadar, Fortinet, and independent researchers. CISA issued a hardening alert on 18 June and updated it on 22 June to incorporate Fortinet's guidance, and the UK NCSC issued a parallel warning, so the steps below now match official government direction rather than researcher recommendation alone.[25][26] They apply regardless of whether an undisclosed vulnerability is later confirmed, because the known attack surface alone justifies them. Any subscriber operating an internet-facing FortiGate firewall or SSL VPN gateway should treat the device as potentially affected until proven otherwise, and given the dataset is now being sold, should act in days rather than weeks.[1][8][10]

Immediate Actions

- Rotate all administrator and SSL VPN credentials now, prioritizing internet-exposed devices and any device involved in a previous credential exposure. Password complexity offers no protection when a credential has already been recovered in plaintext, so rotation, not strengthening, is the operative control.[1][10]
- Remove the FortiGate management interface from direct public internet exposure and restrict it to trusted internal networks. Management-interface exposure characterizes a majority of affected devices and is the single most effective reduction in attack surface.[5][10]
- Enforce multi-factor authentication on every administrative and remote-access account, so that a recovered password alone does not grant access.[8][10]

Configuration and Patch Hygiene

- Upgrade to a supported FortiOS version, then require every administrator to log in at least once after the upgrade to force re-hashing to PBKDF2. The migration does not take effect for an administrator until that administrator logs in.[10][8]
- Where a re-login is not feasible, manually reset remaining administrator passwords using a super_admin account to trigger PBKDF2 hashing.[8][10]
- Disable FortiCloud SSO administrative login unless it is operationally required, since CVE-2026-24858 compromised even fully patched devices where SSO was enabled. Verify the Allow administrative login using FortiCloud SSO setting.[12][15]

Detection and Response

- Review device login history for unfamiliar access by time, source location, or account, and audit the configuration for unauthorized local administrator accounts or VPN changes consistent with the observed CVE-2026-24858 behavior.[1][12]
- Where indicators of compromise are present, treat the device as breached: restore configuration from a known-clean version and engage incident response to assess lateral movement into internal networks. Because the exposed data includes Kerberos hashes and not only device credentials, rotation must extend beyond the firewall to all Active Directory accounts, not just the LDAP or service accounts the device directly touches. Treat the compromise as a potential domain compromise, not only a perimeter one.[8][14][24][29]
- Check the organization's domains against the free lookup tools published by Hudson Rock and SOCRadar to determine whether the organization appears in the dataset, treating any appearance as a strong indicator of compromise rather than a benign listing.[1][6]

Decision Support

The most time-sensitive decision for any subscriber operating internet-facing Fortinet devices is credential rotation paired with management-interface withdrawal, executed in the next several days rather than queued behind a patch cycle, because the credential set is already validated and the cost of inaction is unauthorized access that may already be in progress. This decision belongs with the Chief Information Security Officer. For financial-services and government subscribers carrying counterparty exposure to affected vendors, the time-sensitive decision is third-party assurance: confirming that material Fortinet-dependent vendors have rotated credentials and withdrawn management exposure. The window for first-mover containment closes as the dataset moves toward wider criminal distribution.[1][5]

SECTION 6: INFORMATION GAPS AND COLLECTION REQUIREMENTS

Two of the four gaps from the prior version have partially closed. Attribution of the core operator is now better characterized as a criminal initial access broker, and the defense-sector compromise has a second, dated source. The following gaps remain open, and we will revise this product as they close.

- The initial access vector. Still the largest gap. Confirmation or exclusion of an undisclosed vulnerability would reshape the patching guidance. Fortinet's 19 June statement attributes the activity to credential reuse and brute force but does not foreclose an undisclosed method on a subset of devices. Collection priority: high.
- Named state attribution of downstream use. Tooling overlap with Volt Typhoon and Salt Typhoon tradecraft is documented, but no party has named a state actor as a buyer or operator of the FortiBleed data. Closing this would move Judgment 6 from tooling overlap toward identification. Collection priority: high.

- Victim or government confirmation of the defense-sector exfiltration, which now rests on two disclosing-research accounts but not on the contractor or a national authority. Collection priority: moderate.
- A fully reconciled device count. SOCRadar has consolidated on 86,644, but the figure remains a disclosing party's number rather than an independently audited total. Collection priority: low.

SECTION 7: SOURCE SUMMARY STATEMENT

This assessment rests on a mix of primary disclosures, vendor and government statements, and reputable secondary security reporting, listed in the endnotes. Source reliability is uneven and is treated as such throughout. The discovery and verification claims by Beaumont and the infrastructure discovery and tooling analysis by SOCRadar are first-order evidence from parties with direct access to the data and a track record in this domain, and carry the most weight. The Fortinet PSIRT statement of 19 June, the CISA alerts of 18 and 22 June, and the CISA and Fortinet detail on CVE-2026-24858 are primary sources at the highest credibility level. Fortinet's statements on the FortiBleed dataset are weighed as those of an interested party with strong incentives to characterize the data as dated. The state-tooling overlap is sourced to Bitsight, and the Volt Typhoon and Salt Typhoon history to Microsoft attribution and government reporting. Scale figures originating from the disclosing researchers are reported as stated and not independently audited by EOTISEC. The defense-sector exfiltration now rests on two disclosing-research accounts and is treated as moderately rather than minimally supported, but not as victim-confirmed.

Source limitations: the initial access vector is unestablished and the device counts are not independently verifiable. The CVSS score for CVE-2026-24858 was reported inconsistently in secondary coverage. A claim of up to 9.8 appears in at least one outlet and is inconsistent with the 9.4 score published by CISA and Fortinet. This report uses the authoritative 9.4 throughout. One numeric discrepancy in the underlying reporting, the 45-versus-48 GPU cracking cluster, is carried as flagged rather than resolved.

SECTION 8: ANALYTIC TRADECRAFT SELF-CERTIFICATION

Requirement	Status
Objectivity: free of advocacy, personal preference, or policy bias	CONFIRMED
Independence of political consideration: no judgment shaped to support a particular outcome	CONFIRMED
Timeliness: source material is current and the report is actionable by the customer	CONFIRMED. Source material current to June 23, 2026
Based on all available sources: gaps documented in Section 6	CONFIRMED
Source credibility described: source quality addressed in Section 7	CONFIRMED
Uncertainty expressed: probability and confidence language conforms to ICD 203 standards	CONFIRMED. Confidence levels stated and differentiated across judgments
Assumptions distinguished from facts: linchpin assumption identified	CONFIRMED. One LINCHPIN ASSUMPTION identified in Section 3
Alternatives incorporated: competing hypotheses addressed	CONFIRMED. Three hypotheses for the access vector in Section 4.6, the state-actor nexus in Section 4.9, and the dated-data alternative in Section 4.10

Requirement	Status
Customer relevance addressed: business impact stated by category	CONFIRMED. Impact in Section 4.8, with recommendations in Section 5
Decision support included: time-sensitive actions, ownership, and cost of inaction	CONFIRMED. Section 5 decision support paragraph
Clear and logical argumentation: main message stated up front in Key Judgments	CONFIRMED
Source verification: primary-source or multi-link corroboration	CONFIRMED. One secondary CVSS error corrected to the CISA value

SECTION 9: ENDNOTES — VERIFIED SOURCE CHAIN

1. SOCRadar. *FortiBleed: The Compromise of 80,000+ Fortinet Firewalls*. Published 16 June 2026, updated 18 June 2026. High credibility. Primary discovery of the operators' infrastructure. https://socradar.io/blog/fortibleed-fortinet-firewalls-compromised/
2. Arctic Wolf. *Active FortiBleed Campaign Impacting Fortinet Devices Across 194 Countries*. High credibility. https://arcticwolf.com/resources/blog/active-fortibleed-campaign-impacting-fortinet-devices-across-194-countries/
3. BleepingComputer. *FortiBleed leak exposes Fortinet VPN credentials for 73,000 devices*. 18 June 2026. High credibility. Beaumont verification quotes and the unknown-vector statement. https://www.bleepingcomputer.com/news/security/fortibleed-leak-exposes-fortinet-vpn-credentials-for-73-000-devices/
4. heise online. *Massive attack on Fortinet firewalls? 74,000 devices affected by FortiBleed*. 18 June 2026. High credibility. Carries the Fortinet statement to TechCrunch. https://www.heise.de/en/news/Massive-attack-on-Fortinet-firewalls-74-000-devices-affected-by-FortiBleed-11336418.html
5. Help Net Security. *74,000 Fortinet firewall credentials exposed in FortiBleed data leak*. 18 June 2026. High credibility. Direct Beaumont quotes on config-export origin. https://www.helpnetsecurity.com/2026/06/18/fortinet-fortibleed-data-leak/
6. BleepingComputer, as in endnote 3, for Diachenko's LinkedIn disclosure, the 1.16 billion FortiGate attempts, and the parallel 2.1 billion MSSQL attempts. https://www.bleepingcomputer.com/news/security/fortibleed-leak-exposes-fortinet-vpn-credentials-for-73-000-devices/
7. CSO Online. *FortiBleed campaign exposes 75,000 Fortinet firewalls worldwide*. High credibility. SOCRadar attribution language and watchTowr commentary. https://www.csoonline.com/article/4186790/fortibleed-campaign-exposes-75000-fortinet-firewalls-worldwide.html
8. CSO Online, as in endnote 7, for Beaumont on impact and the unknown initial access vector. https://www.csoonline.com/article/4186790/fortibleed-campaign-exposes-75000-fortinet-firewalls-worldwide.html
9. Security Affairs. *FortiBleed Exposes Admin Passwords for 75,000 Fortinet Firewalls*. 18 June 2026. High credibility. Config decryption via serial number and the Belsen IP comparison. https://securityaffairs.com/193817/hacking/fortibleed-exposes-admin-passwords-for-75000-fortinet-firewalls.html
10. Arctic Wolf, as in endnote 2, for FortiOS PBKDF2 versions 7.2.11, 7.4.8, 7.6.1, the post-upgrade re-login requirement, and the retained old-password hash. https://arcticwolf.com/resources/blog/active-fortibleed-campaign-impacting-fortinet-devices-across-194-countries/
11. Kevin Beaumont, DoublePulsar. *FortiBleed: 75k Fortinet firewalls have admin passwords cracked*. 17 June 2026. Primary analysis, cited via corroborating reporting where the original was not directly

retrievable. https://doublepulsar.com/fortibleed-75k-fortinet-firewalls-have-admin-passwords-cracked-60299faa65f8

12. CISA. *Fortinet Releases Guidance to Address Ongoing Exploitation of Authentication Bypass Vulnerability CVE-2026-24858*. 28 January 2026. Highest credibility. CWE-288, CVSS 9.4, KEV listing. https://www.cisa.gov/news-events/alerts/2026/01/28/fortinet-releases-guidance-address-ongoing-exploitation-authentication-bypass-vulnerability-cve-2026
13. The Hacker News. *Fortinet Patches CVE-2026-24858 After Active FortiOS SSO Exploitation Detected*. Confirms the 27 January 2026 advisory and 30 January federal deadline. https://thehackernews.com/2026/01/fortinet-patches-cve-2026-24858-after.html
14. Triskele Labs. *Critical Fortinet FortiCloud SSO Authentication Bypass Under Active Exploitation CVE-2026-24858*. On observed configuration theft and persistence behavior. https://www.triskelelabs.com/blog/critical-fortinet-forticloud-sso-authentication-bypass-under-active-exploitation-cve-2026-24858
15. CyberDesserts. *CVE-2026-24858: The Fortinet Patch That Wasn't*. On patched devices compromised and the Shadowserver SSO-enabled device count falling below 10,000. https://blog.cyberdesserts.com/cve-2026-24858-fortinet-sso-bypass/
16. Help Net Security. *Configuration files for 15,000 Fortinet firewalls leaked*. 16 January 2025 (Belsen Group). https://www.helpnetsecurity.com/2025/01/16/leaked-fortinet-fortigate-configs-vpn-credentials-ip-list/
17. Dark Reading. *15K Fortinet Device Configs Leaked to the Dark Web*. 17 January 2025. On CVE-2022-40684 and CVE-2018-13379 as the Belsen sources. https://www.darkreading.com/endpoint-security/15k-fortinet-device-configs-leaked-dark-web
18. SecurityWeek. *Data From 15,000 Fortinet Firewalls Leaked by Hackers*. 16 January 2025. On the October 2022 collection date and the CVE-2022-40684 zero-day timeline. https://www.securityweek.com/data-from-15000-fortinet-firewalls-leaked-by-hackers/
19. The Register. *Fortinet: FortiGate config leaks are genuine but misleading*. 17 January 2025. On Fortinet's dated-data framing and the December 2024 Arctic Wolf campaign. https://www.theregister.com/2025/01/17/fortinet_fortigate_config_leaks/
20. Censys. *Massive FortiGate Config Leak: Assessing the Impact*. On 15,469 hosts with over half still online and the 2021 leak of nearly 500,000 VPN credentials. https://censys.com/blog/fortigate-config-leak-impact/
21. Rapid7. *Critical Vulnerabilities in Fortinet CVE-2025-59718, CVE-2025-59719 Exploited in the Wild*. On admin authentication followed by immediate configuration download. https://www.rapid7.com/blog/post/etr-critical-vulnerabilities-in-fortinet-cve-2025-59718-cve-2025-59719-exploited-in-the-wild/
22. SOC Prime. *CVE-2026-24858: FortiOS SSO Zero-Day Exploited in the Wild*. On the two malicious FortiCloud accounts blocked 22 January and SSO suspension 26 January 2026. https://socprime.com/blog/cve-2026-24858-vulnerability/
23. MITRE ATT&CK, External Remote Services (T1133), citing NSA, CISA, FBI, NCSC. *Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments*. July 2021. https://attack.mitre.org/techniques/T1133/
24. The CyberSec Guru. *FortiBleed: How 75,000 Fortinet Firewalls Were Silently Compromised in 2026*. On the reported four fully compromised organizations and the Turkish NATO contractor claim. https://thecybersecguru.com/news/fortibleed-fortinet-firewall-credential-leak/
25. Fortinet PSIRT (Carl Windsor). *Analysis of Reported Credential Compromise of FortiGate Devices: What you need to know about FortiBleed*. 19 June 2026. Highest credibility. Primary vendor statement. Internal advisories FG-IR-26-060 and FG-IR-25-647. Not a new vulnerability. https://www.fortinet.com/blog/psirt-blogs/analysis-of-reported-credential-compromise-of-fortigate-devices
26. CISA. *CISA Urges Hardening Fortinet Devices After Reports of Credential Exposure*. 18 June 2026, updated 22 June 2026. Highest credibility. Primary government alert. Session termination and

credential reset guidance. https://www.cisa.gov/news-events/alerts/2026/06/18/cisa-urges-hardening-fortinet-devices-after-reports-credential-exposure

27. Huntress. *2026-June FortiBleed Credential Exposure*. High credibility. 845 partner organizations identified as affected. Exposed data included cleartext credentials and Kerberos hashes. Full AD rotation advised. https://support.huntress.io/hc/en-us/articles/52698652545171-2026-June-Fortibleed-Credential-Exposure
28. Cyber Security News. *Hackers Using FortigateSniffer Tool That Turns Compromised Firewalls Into Password Collectors.* 23 June 2026. High credibility, reporting SOCRadar STRU. Named tooling fg_sniffer. 260 servers, 659 harvest cycles, and a 15 June DFS-over-SMB exfiltration after cracking 172 Kerberos RC4 hashes. https://cybersecuritynews.com/fortigatesniffer-tool-fortibleed/
29. Bitsight. *Security Alert: FortiBleed Fortinet VPN Credentials and Firewall Exposed*. High credibility. Active sale on a Russian cybercrime forum. Chisel and Neo-reGeorg tunneling tools tied to the activity, previously seen in Volt Typhoon. Two-tier criminal and sophisticated-actor use. https://www.bitsight.com/blog/security-alert-fortibleed-fortinet-vpn-credentials-firewall-exposed
30. Palo Alto Networks Unit 42, via Mallory threat-brief aggregation. *Credential-Harvesting Campaign Compromises 30,000 Fortinet Firewalls*. High credibility for the Unit 42 and SpyCloud findings. Initial access broker on Exploit.in claimed responsibility 16 June (unvalidated by Unit 42). SpyCloud dated the operation to 19 May. https://www.mallory.ai/stories/019ed5b0-62d5-772e-91c2-78fa18a7429f
31. IBM X-Force. *Palo Alto and Fortinet Secure Remote Access Gateway / VPN Compromise Advisory*. 19 June 2026. High credibility. Edge-access compromise as a pathway into internal identity systems, including AD pivot. Patching does not invalidate stolen credentials. Note: the Palo Alto CVE-2026-0257 detail in this advisory is a separate product incident and is not part of FortiBleed. https://www.ibm.com/think/x-force/palo-alto-fortinet-secure-remote-access-gateway-vpn-compromise-advisory
32. NJCCIC and Microsoft attribution. *Volt Typhoon Threat Profile*. On the China-linked Guam critical-infrastructure campaign directed against FortiGate appliances, attributed by Microsoft in 2023. https://www.cyber.nj.gov/threat-landscape/nation-state-threat-analysis-reports/china-linked-cyber-operations-targeting-us-critical-infrastructure/volt-typhoon
33. Fortinet FortiGuard Labs and Tenable. *Salt Typhoon Threat Actor Profile*. On the China-linked group, active since 2019, exploiting Fortinet among other edge vendors for espionage against telecommunications and government targets. https://fortiguard.fortinet.com/threat-actor/5557/salt-typhoon
34. Industrial Cyber, summarizing a 2026 Congressional Research Service report. *State-Sponsored Exploitation of Fortinet and Microsoft Exchange Flaws*. On China, Russia, Iran, and North Korea as the most active state actors and the Volt and Salt Typhoon critical-infrastructure cases. https://industrialcyber.co/reports/iranian-state-sponsored-hackers-exploit-microsoft-exchange-fortinet-flaws-to-access-us-infrastructure-networks-crs-finds/