INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-08 13:49 UTC

Security Advisory - Action Required - Active Exploitation of Check Point VPN Authentication Bypass (CVE-20 ...

CVE VULNERABILITY | CRITICAL

SCC Item ID	SCC-CVE-2026-0273
Type	CVE Vulnerability
CVE ID	CVE-2026-50751
Severity	CRITICAL
EPSS Score	0.0001 (1th percentile)
Affected Products	Check Point Remote Access VPN / Security Gateway (specific versions unconfirmed from available sources)
Published	13 hours ago
Discovery Source	Serper

Executive Summary

A security advisory is circulating that references CVE-2026-50751, described as a critical authentication bypass affecting Check Point Remote Access VPN products. Source verification reveals significant data quality problems: no NVD or CISA KEV entry exists for CVE-2026-50751 despite the identifier following valid 2026 calendar-year numbering, and the linked sources primarily document CVE-2024-24919, a separate but related Check Point VPN vulnerability confirmed exploited in 2024. Organizations running Check Point Remote Access VPN should treat this as a signal to verify patch status against CVE-2024-24919 while CVE-2026-50751 is independently verified through official channels.

Technical Analysis

INTEGRITY NOTICE: CVE-2026-50751 cannot be verified. No NVD entry, no CISA KEV entry, no VulnCheck KEV entry, and no vendor advisory was confirmed for this identifier. All linked sources, including Check Point support article sk182336, address CVE-2024-24919, a distinct information disclosure and authentication bypass vulnerability in Check Point Remote Access VPN / Security Gateway that was actively exploited beginning May 2024. CVE-2024-24919 is documented under CWE-287 (Improper Authentication) and CWE-306 (Missing Authentication for Critical Function), matching the CWE data provided. MITRE ATT&CK techniques T1133 (External Remote Services), T1190 (Exploit Public-Facing Application), and T1078 (Valid Accounts) are consistent with the exploitation pattern observed in CVE-2024-24919 campaigns. CVSS base score for

CVE-2026-50751 is 0.0 (unscored); EPSS is 0.0001 (0.01th percentile), reflecting no established scoring data. Operators should apply Check Point's preventative hotfix documented in sk182336 for CVE-2024-24919 and monitor for further official advisories that may clarify or supersede the CVE-2026-50751 identifier.

Action Checklist

1. Step 1: Containment, Identify all Check Point Remote Access VPN / Security Gateway instances exposed to the internet. Cross-reference against Check Point sk182336 to determine whether the CVE-2024-24919 hotfix has been applied. Until the CVE-2026-50751 identifier is independently confirmed via NVD or a Check Point official advisory, treat CVE-2024-24919 patch status as the actionable baseline. Restrict VPN gateway management interfaces to trusted IP ranges if not already enforced (NIST AC-17).
2. Step 2: Detection, Query VPN gateway authentication logs for anomalous successful authentications with no corresponding MFA event, authentication attempts against accounts not in active directory, or access from unexpected geographic sources. Review logs for exploitation indicators consistent with T1190 (public-facing application exploitation) and T1078 (valid account abuse). Enable audit logging per NIST AU-2 and AU-12 if not already active. CIS 8.2 requires audit log collection to be confirmed across all affected gateway assets.
3. Step 3: Eradication, Apply the Check Point hotfix documented in sk182336 for CVE-2024-24919 immediately if not already applied. Do not delay this patching while waiting for CVE-2026-50751 verification. Monitor NVD (https://nvd.nist.gov) for any official entry under CVE-2026-50751; do not apply advisories specific to CVE-2026-50751 until verified by Check Point or NVD. No mapped control for CVE-2026-50751-specific remediation; identifier is unverified.
4. Step 4: Recovery, After patching, validate that all VPN gateway authentication flows require MFA (NIST AC-7; D3-MFA). Rotate credentials for any accounts that authenticated through the affected VPN gateway during the exposure window (D3-CRO). Review account activity logs for lateral movement indicators consistent with T1078. Confirm audit logging is intact and forwarding to SIEM (NIST AU-9).
5. Step 5: Post-Incident, Conduct a gap assessment against NIST AC-6 (Least Privilege) and AC-3 (Access Enforcement) for VPN-authenticated user sessions. Evaluate whether your threat intelligence pipeline can detect anomalous CVE identifiers (unverified, missing from NVD) before they are actioned; this advisory demonstrates a data quality risk in upstream feeds. Document the CVE-2026-50751 identifier as unverified in your vulnerability tracking system pending official confirmation.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal/privacy counsel if SmartLog or AD event logs show any successful VPN authentication during the CVE-2024-24919 exposure window followed by access to systems storing PII, PHI, or payment card data — triggering breach notification assessment under applicable regulations (GDPR 72-hour window, HIPAA 60-day, state breach laws) — or if the CVE-2026-50751 identifier receives an official NVD entry with a CVSS score above 9.0 or appears on the CISA KEV catalog, which would require immediate re-triage to 'immediate' priority.

Recovery Notes	After applying sk182336 and rotating exposed credentials, monitor Check Point SmartLog and AD authentication events for a minimum of 30 days for re-appearance of the source IPs and user accounts identified during the exposure window analysis — threat actors who harvested credentials via CVE-2024-24919 have demonstrated dwell times of weeks before pivoting, as observed in 2024 exploitation campaigns. Validate that VPN-authenticated sessions post-recovery consistently show MFA events paired with each authentication success in SmartLog before closing the incident. Retain all captured log evidence for a minimum of 12 months given potential regulatory inquiry timelines, consistent with NIST AU-11 (Audit Record Retention) requirements.
Forensic Artifacts	Check Point gateway HTTP access logs ($FWDIR/log/ or embedded web server path) containing URI requests with path traversal sequences (e.g., '../../etc/passwd', '/clients/MyCRL') — the CVE-2024-24919 exploit mechanism is an unauthenticated path traversal in the Mobile Access / Remote Access VPN web component, and these sequences are the primary exploitation fingerprint. | Check Point SmartLog VPN authentication records filtered for the period from sk182336 publication (May 2024) to hotfix application date, specifically events where 'Authentication Method' does not include a second factor — accounts authenticated using credentials potentially stolen via the path traversal would appear as single-factor successes. | Active Directory Security Event Log (Event IDs 4624, 4648, 4768, 4769) on domain controllers, filtered to source IPs within the Check Point gateway's VPN Office Mode IP pool, for the same exposure window — post-exploitation lateral movement using harvested VPN credentials (T1078) would produce Kerberos ticket requests and network logon events originating from these IPs. | Contents of $FWDIR/conf/ directory captured pre-patch, specifically any files readable by the Check Point web process user context — CVE-2024-24919 allowed unauthenticated read of files accessible to the gateway's web service, potentially including password hashes, API keys, or LDAP bind credentials stored in Check Point configuration. | Network flow or firewall logs showing outbound connections from the Check Point gateway's management IP or VPN client IP pool to external IPs during the exposure window — successful exploitation followed by credential use for lateral movement or data exfiltration would appear as unusual outbound sessions from internal hosts newly reachable via the VPN tunnel.

Per-Action IR Details

Step 1: Containment — Identify all Check Point Remote Access VPN / Security Gateway instances exposed to the internet. Cross-reference against Check Point sk182336 to determine whether the CVE-2024-24919 hotfix has been applied. Until the CVE-2026-50751 identifier is independently confirmed via NVD or a Check Point official advisory, treat CVE-2024-24919 patch status as the actionable baseline. Restrict VPN gateway management interfaces to trusted IP ranges if not already enforced (NIST AC-17).

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Use 'cpinfo -y all' and 'fw stat' on each Check Point gateway to enumerate exposed interfaces and confirm hotfix build levels against sk182336 without a CMDB. For management interface restriction, apply a Check Point host access rule in SmartConsole limiting GUI/API access (TCP 18190, 19009) to jump-host IP ranges only. Two-person task: one runs asset enumeration, one applies the access restriction rule and installs policy.

Evidence: Before restricting access, capture: (1) Check Point SmartLog or $FWDIR/log/*.log* files showing all VPN authentication events in the 30 days preceding this action — CVE-2024-24919 is a path traversal allowing unauthenticated file read of /etc/passwd and sensitive config files, so look for HTTP GET requests to /clients/MyCRL or similar traversal paths in the gateway's httpd access log at $FWDIR/log/https_inspection/; (2) 'netstat -an' output from

each gateway capturing all established connections to TCP 443 and TCP 18191 (IKE/VPN) at the time of containment; (3) snapshot of currently active VPN tunnels via 'vpn tu' or SmartView Monitor before any policy changes sever active sessions.

Step 2: Detection — Query VPN gateway authentication logs for anomalous successful authentications with no corresponding MFA event, authentication attempts against accounts not in active directory, or access from unexpected geographic sources. Review logs for exploitation indicators consistent with T1190 (public-facing application exploitation) and T1078 (valid account abuse). Enable audit logging per NIST AU-2 and AU-12 if not already active. CIS 8.2 requires audit log collection to be confirmed across all affected gateway assets.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, run this on the Check Point gateway or a log collector: grep the SmartLog export (CSV or syslog forward) for authentication events where 'Authentication method' is 'Certificate' or 'Password' and no corresponding RADIUS/MFA accept record exists within a 60-second window — CVE-2024-24919 exploitation can result in credential material extracted from config files being used to authenticate without triggering MFA challenges. Use the following on a Linux syslog receiver: 'grep -E "VPN.*Authentication succeeded" /var/log/checkpoint.log | awk "{print $1,$2,$3,$9,$11}" | sort | uniq -c | sort -rn' to surface high-frequency auth successes by source IP. Cross-check source IPs against a free geo-IP lookup (db-ip.com offline CSV) in a bash loop for unexpected countries.

Evidence: Capture before analysis: (1) Check Point SmartLog filtered for Event Type 'VPN Authentication' and 'Login' for the full window since sk182336 hotfix release date (May 2024) — CVE-2024-24919 exploitation has been observed leading to credential harvesting and subsequent valid-account VPN access (T1078); (2) $FWDIR/conf/vpn.conf and $FWDIR/conf/objects_5_0.C to identify which authentication schemes (certificate, password, RADIUS) were active — the path traversal in CVE-2024-24919 targets files readable by the Check Point web process, so presence of unexpected file-read attempts in httpd logs is a primary indicator; (3) Windows Security Event Log Event ID 4624 (Logon Type 3/10) on AD domain controllers for accounts whose credentials may have been exposed via the traversal, filtered to the VPN gateway source IP.

Step 3: Eradication — Apply the Check Point hotfix documented in sk182336 for CVE-2024-24919 if not already applied. Monitor the Check Point Security Advisory portal and NVD (https://nvd.nist.gov) for any official entry under CVE-2026-50751 before applying advisories specific to that identifier. Do not apply unofficial patches or guidance referencing CVE-2026-50751 until verified by Check Point or NVD. No mapped control for CVE-2026-50751-specific remediation — identifier is unverified.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Download the sk182336 hotfix directly from CheckPoint's User Center (requires support account) and verify the SHA256 checksum published in the SK before installation — do not accept hotfix binaries from third-party sources given the unverified advisory circulating for CVE-2026-50751. Run 'cpinfo -y all > pre_patch_cpinfo.txt' before applying to preserve pre-patch state for comparison. After hotfix installation, run 'cpvinfo $FWDIR/bin/vpnd | grep -i version' and compare build number to sk182336's fixed build table to confirm successful application. Two-person verification: one applies, one independently confirms build string.

Evidence: Before patching, preserve: (1) Full copy of $FWDIR/conf/ directory — CVE-2024-24919's path traversal can expose password hashes or cleartext credentials stored in Check Point configuration files (specifically files accessible via the Mobile Access portal web process), and this directory state is needed to determine what was readable if exploitation occurred; (2) Web process access logs at /var/log/httpd2_error.log or Check Point's embedded web server log path showing any HTTP requests containing '../' traversal sequences targeting /etc/shadow, /etc/passwd, or Check Point-specific credential stores; (3) md5sum or sha256sum of key binaries ($FWDIR/bin/vpnd, $FWDIR/bin/fwd)

pre-patch to document pre-remediation state for any future forensic comparison.

Step 4: Recovery — After patching, validate that all VPN gateway authentication flows require MFA (NIST AC-7; D3-MFA). Rotate credentials for any accounts that authenticated through the affected VPN gateway during the exposure window (D3-CRO). Review account activity logs for lateral movement indicators consistent with T1078. Confirm audit logging is intact and forwarding to SIEM (NIST AU-9).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-2 (Account Management), NIST AU-9 (Protection Of Audit Information), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: For MFA validation without a commercial solution, audit Check Point SmartConsole Remote Access Community settings to confirm 'Authentication' is set to a two-factor method (Certificate + Password, or RADIUS with MFA provider) and that 'Office Mode' IP assignment only completes after both factors succeed — review this in the gateway's VPN community properties. For credential rotation tracking in environments without PAM tooling, generate a list of all accounts with successful VPN authentications during the exposure window using SmartLog export, then script AD password resets via PowerShell: 'Get-ADUser -Filter * | Where-Object {$_.SamAccountName -in $exposedAccounts} | Set-ADAccountPassword -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "TempP@ss!" -Force)' followed by forcing change at next logon.

Evidence: Before marking recovered: (1) Windows Security Event Log Event ID 4648 (Explicit Credential Logon) and 4768/4769 (Kerberos TGT/TGS requests) from domain controllers, filtered to source IPs associated with the VPN gateway's Office Mode IP pool — post-exploitation lateral movement via T1078 using harvested credentials would appear here; (2) Check Point SmartLog 'Blade: VPN' records showing session duration, bytes transferred, and accessed internal resources for all sessions during the exposure window — anomalously long sessions or high data transfer volumes may indicate data staging; (3) Confirmation screenshot or log export showing AU-9-compliant log forwarding is active (syslog to remote collector, not only local storage) so log tampering on the gateway itself cannot eliminate the audit trail.

Step 5: Post-Incident — Conduct a gap assessment against NIST AC-6 (Least Privilege) and AC-3 (Access Enforcement) for VPN-authenticated user sessions. Evaluate whether your threat intelligence pipeline can detect anomalous CVE identifiers (future-dated, misformatted) before they are actioned — this advisory demonstrates a data quality risk in upstream feeds. Document the CVE-2026-50751 identifier as unverified in your vulnerability tracking system pending official confirmation.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST AC-6 (Least Privilege), NIST AC-3 (Access Enforcement), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For TI feed data quality validation without a commercial TIP, implement a lightweight CVE identifier sanity check in your intake process: a simple regex pattern '^CVE-(199[6-9]|20[0-2][0-9])-[0-9]{4,}$' against current year will flag future-dated identifiers like CVE-2026-50751 before they are acted upon — implement as a Python pre-processing script or a Sigma detection rule against your log ingestion pipeline. For the AC-6 gap assessment on VPN sessions, export the SmartLog VPN session data and compare accessed internal resources per user against their documented role in AD group membership — flag any VPN user who accessed more than three internal subnets not associated with their department.

Evidence: For the lessons-learned record: (1) Preserve the original advisory referencing CVE-2026-50751 in its received form (email headers, feed API response, or STIX/TAXII object) to document provenance and support TI feed vendor feedback; (2) Export the full timeline of internal actions taken in response to this advisory — from receipt to containment decisions — to quantify MTTD and MTTR against a CVE that turned out to be unverified, establishing a baseline for TI quality impact on response cost; (3) Document the NVD and CISA KEV negative lookup results (screenshots with timestamps) for CVE-2026-50751 as evidence supporting the 'unverified' classification in your

vulnerability tracking system, in the event the identifier is later officially assigned with different scope or severity than the circulating advisory claimed.

Detection Guidance

Because CVE-2026-50751 is unverified, detection guidance is anchored to CVE-2024-24919 exploitation patterns, which the source data explicitly links. Detection focus areas: (1) Authentication anomalies, search VPN gateway logs for successful authentications that bypass MFA, particularly against accounts inactive for 30+ days (CIS 5.3 dormant accounts); correlate with D3-LAM (Local Account Monitoring) for local account misuse. (2) Account enumeration, log queries for repeated authentication attempts against non-existent or disabled accounts per NIST AC-7 (Unsuccessful Logon Attempts). (3) Unusual session origins, flag VPN sessions originating from Tor exit nodes, anonymizing proxies, or geographic regions inconsistent with baseline user behavior. (4) Post-auth behavior, monitor for rapid internal reconnaissance or credential access activity immediately following VPN authentication, consistent with T1078 (Valid Accounts) and T1133 (External Remote Services) abuse. SIEM rule suggestions: alert on successful VPN auth followed by no subsequent internal activity within 60 seconds (potential automated access); alert on VPN auth events with missing or null MFA fields. No confirmed IOC patterns for CVE-2026-50751 are available from verified sources. For confirmed CVE-2024-24919 exploitation indicators, consult CISA advisories, VulnCheck, or Check Point threat intelligence feeds.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`CVE-2026-50751 — no confirmed IOCs available`	CVE identifier is unverified; no NVD entry, no confirmed exploit traffic, no threat actor attribution. IOC list will remain empty until the identifier is confirmed by Check Point or NVD.	LOW

Framework Mappings

MITRE-ATTACK

- **T1133** — External Remote Services
- **T1190** — Exploit Public-Facing Application
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CA-8** — Penetration Testing

- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-4** — System Monitoring
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1133	External Remote Services	Persistence
T1190	Exploit Public-Facing Application	Initial-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
	https://blog.checkpoint.com/security/check-point-releases-important...	T3
(consolidated)	https://thehackernews.com/2026/06/critical-check-point-vpn-flaw-exp...	T3
(consolidated)	https://www.techzine.eu/news/security/141933/check-point-warns-of-c...	T3
sk182336 - Preventative Hotfix for CVE-2024-24919	https://support.checkpoint.com/results/sk/sk182336	T3
Advisory: Check Point Remote Access VPN vulnerability (CVE-2024 ...	https://www.mnemonic.io/resources/blog/advisory-check-point-remote-...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-50751	T1

Generated 2026-06-08 13:49 UTC by TJS Security Command Center