INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 19:20 UTC

Active Exploitation of Three Critical Fortinet FortiSandbox Vulnerabilities (CVE-2026-39813, CVE-2026-39808, CVE-2026-25089)

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0312
Type	CVE Vulnerability
CVE ID	CVE-2026-39813, CVE-2026-39808, CVE-2026-25089
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.2364 (98th percentile)
Affected Products	Fortinet FortiSandbox (on-premise), FortiSandbox Cloud, FortiSandbox PaaS, all deployment types affected; specific version ranges not confirmed from available sources
Published	2026-06-16T06:30:41
Discovery Source	Rss

Executive Summary

Three critical vulnerabilities in Fortinet FortiSandbox are under active exploitation (as reported by secondary sources; vendor confirmation pending), affecting on-premise, cloud, and PaaS deployments. Unauthenticated attackers can execute arbitrary commands or bypass authentication, enabling unauthorized access to FortiSandbox management and analysis functions. Organizations running FortiSandbox in any deployment mode face immediate risk of security infrastructure compromise, which could blind defenders to malware activity across the enterprise.

Technical Analysis

Three critical vulnerabilities affect Fortinet FortiSandbox across all deployment types (on-premise, cloud, PaaS). CVE-2026-39813 (CWE-22, path traversal) and CVE-2026-39808 (CWE-78, OS command injection) enable unauthenticated remote command execution via crafted HTTP requests. CVE-2026-25089 (CWE-306, missing authentication for critical function) allows authentication bypass; this CVE was patched only days before active exploitation was confirmed, indicating a near-zero patch-to-exploit window and probable pre-patch adversary knowledge. CVSS base score: 9.5. EPSS score: 0.236 (97.5th percentile), indicating very high exploitation probability relative to the broader CVE population. MITRE ATT&CK techniques mapped: T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), T1078.001 (Valid Accounts: Default

Accounts), T1133 (External Remote Services), T1562.001 (Impair Defenses: Disable or Modify Tools), T1203 (Exploitation for Client Execution). Fortinet FortiSandbox (on-premise, cloud, PaaS), all deployment types affected. Specific patched version numbers not yet confirmed from available sources; assume all versions unpatched until Fortinet PSIRT advisory is released. Active exploitation is reported by secondary-tier sources; CISA KEV listing and Fortinet PSIRT advisory confirmation are pending as of this writing. Source quality score: 0.712. Corroboration from a Fortinet PSIRT advisory or CISA KEV addition would raise confidence to highest tier.

Action Checklist

1. Step 1: Containment. Immediately restrict network access to all FortiSandbox management interfaces (on-premise, cloud, and PaaS). Place FortiSandbox behind a WAF or restrict ingress to known administrative IP ranges. Block inbound HTTP/HTTPS to FortiSandbox from untrusted networks at the perimeter firewall. Reference: NIST AC-17 (Remote Access), establish and enforce connection requirements for all remote-accessible management planes.
2. Step 2: Detection. Review FortiSandbox web server and authentication logs for anomalous HTTP requests, particularly those containing path traversal sequences (e.g., '../' patterns) or unexpected command characters in request parameters. Hunt for unauthenticated sessions accessing administrative functions (CWE-306 pattern). Correlate with SIEM for T1190 and T1059 indicators. Enable verbose access logging if not already active per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). Query for process spawning from web server processes, which would indicate successful OS command injection (CVE-2026-39808).
3. Step 3: Eradication. Apply Fortinet's official patches for CVE-2026-39813, CVE-2026-39808, and CVE-2026-25089 as published in the Fortinet PSIRT advisory. Await Fortinet's official PSIRT advisory at https://www.fortiguard.com/psirt; if patches are not yet available, contact Fortinet support for patch availability confirmation and affected version ranges specific to your deployment. If patches are not yet available for your version, implement vendor-recommended workarounds. Reference: NIST SI-2 (Flaw Remediation); CIS 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery. After patching, rotate all FortiSandbox administrative credentials and API keys, as authentication bypass (CVE-2026-25089) may have permitted unauthorized access prior to remediation. Verify patch application against the Fortinet advisory version table. Monitor FortiSandbox for anomalous process execution and unexpected outbound connections for a minimum of 14 days post-remediation. Reference: D3-CRO (Credential Rotation); NIST AU-6 (Audit Record Review, Analysis, and Reporting).
5. Step 5: Post-Incident. Conduct a review of patch management SLAs for critical security infrastructure. CVE-2026-25089 demonstrates that threat actors may possess pre-patch knowledge, requiring patch application windows measured in hours, not days, for critical security tooling. Implement compensating controls per NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) to limit blast radius if a security appliance is compromised. Evaluate whether FortiSandbox management interfaces were exposed to the internet and remediate that exposure regardless of patch status.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to CISO, legal counsel, and external IR retainer immediately if forensic analysis confirms successful exploitation of CVE-2026-25089 (authentication bypass) — specifically, if unauthorized admin sessions, rogue accounts, or evidence of FortiSandbox verdict manipulation are found — as compromise of the sandbox infrastructure means the organization's malware detection capability was potentially blinded during the dwell period, requiring breach notification assessment for any regulated data environments monitored by FortiSandbox during that window.
Recovery Notes	After patching, verify FortiSandbox is running the Fortinet-confirmed patched firmware version by comparing `get system status` output against the specific fixed-version table in the Fortinet PSIRT advisory for CVE-2026-39813, CVE-2026-39808, and CVE-2026-25089 before returning the appliance to production malware analysis duties. For 14 days post-remediation, maintain elevated monitoring of all outbound connections from the FortiSandbox host and audit logs for any admin account activity, process execution anomalies, or API calls that deviate from the appliance's normal operational baseline — active exploitation prior to patching may have left a persistent implant that survives firmware update if it was written to persistent storage. Any malware submissions processed by FortiSandbox during the confirmed or suspected compromise window should be treated as potentially unanalyzed or manipulated and re-submitted through an uncompromised analysis channel.
Forensic Artifacts	FortiSandbox web server access logs (typically /var/log/fortiSandbox/access.log or equivalent appliance log path): search for HTTP requests containing path traversal sequences (../, %2e%2e%2f), shell metacharacters ($(), ;, |, backtick) in URI parameters, or direct requests to administrative API endpoints from IPs with no prior authenticated session — artifacts of CVE-2026-39808 (OS command injection) and CVE-2026-39813 exploitation attempts | FortiSandbox authentication audit logs: look for HTTP 200 or 302 responses to /api/ or /admin/ endpoints associated with source IPs that have zero corresponding successful login events — the definitive log pattern for CVE-2026-25089 authentication bypass exploitation | OS-level process creation records (auditd execve events or Sysmon Event ID 1 on any Windows FortiSandbox component): child processes with parent process name matching the FortiSandbox web daemon (httpd, nginx, or the FortiSandbox application service) that resolve to shells (sh, bash, python, cmd.exe, powershell.exe) are high-confidence indicators of successful CVE-2026-39808 remote OS command injection | FortiSandbox admin account configuration state (output of 'config system admin; show' and 'config system api-user; show' captured pre-rotation): any admin account or API user not present in the pre-incident CIS 5.1 account inventory baseline is a strong indicator of attacker-created persistence following successful authentication bypass via CVE-2026-25089 | Outbound network connection logs from the FortiSandbox host (firewall egress logs or tcpdump captures), particularly DNS queries and TCP sessions to non-Fortinet-owned infrastructure initiated by the FortiSandbox process after the earliest confirmed anomalous inbound request — these represent potential C2 beaconing or data exfiltration following successful RCE via CVE-2026-39808 or CVE-2026-39813

Per-Action IR Details

Step 1: Containment — Immediately restrict network access to all FortiSandbox management interfaces (on-premise, cloud, and PaaS). Place FortiSandbox behind a WAF or restrict ingress to known administrative IP ranges. Block inbound HTTP/HTTPS to FortiSandbox from untrusted networks at the perimeter firewall. Reference: NIST AC-17 (Remote Access) — establish and enforce connection requirements for all remote-accessible management planes.

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 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On a 2-person team without a managed WAF, immediately apply a host-based IPTables or Windows Firewall rule on the FortiSandbox host to accept TCP 443/80 only from your documented admin IP ranges. Example (Linux): `iptables -I INPUT -p tcp --dport 443 ! -s -j DROP`. For cloud deployments, apply a Security Group or NSG deny-all inbound rule on ports 443/80 from 0.0.0.0/0 immediately via cloud console. Verify block is in place with `curl -k https://` from an untrusted IP — connection should time out.

Evidence: Before restricting network access, capture current active connections to the FortiSandbox management interface to document whether exploitation has already occurred: run `ss -tnp` or `netstat -ano` on the FortiSandbox host to record all established TCP sessions on ports 443 and 80. Export FortiSandbox web server access logs (typically under `/var/log/fortiSandbox/` or the equivalent appliance log path) for the 72-hour window preceding this action, preserving originating IP addresses of any unauthenticated or anomalous management-plane requests. Capture a list of currently authenticated admin sessions from the FortiSandbox GUI (System > Admin Sessions) or CLI (`diagnose sys session list`) before sessions are terminated by the firewall rule. These volatile session records are destroyed the moment network access is blocked.

Step 2: Detection — Review FortiSandbox web server and authentication logs for anomalous HTTP requests, particularly those containing path traversal sequences (e.g., '../' patterns) or unexpected command characters in request parameters. Hunt for unauthenticated sessions accessing administrative functions (CWE-306 pattern). Correlate with SIEM for T1190 and T1059 indicators. Enable verbose access logging if not already active per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). Query for process spawning from web server processes, which would indicate successful OS command injection (CVE-2026-39808).

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 a SIEM, use grep or awk directly against FortiSandbox web server access logs to hunt for path traversal and injection patterns: `grep -E '(\.\./|%2e%2e%2f|;|\$\(|\`|\|)' /var/log/fortiSandbox/access.log`. For process injection evidence from CVE-2026-39808 (OS command injection), deploy Sysmon on any Windows-based FortiSandbox component and filter Event ID 1 (Process Create) for child processes parented by the web server process (e.g., `httpd`, `nginx`, or the FortiSandbox daemon). On Linux, use `auditd` with a rule watching for `execve` calls from the web server process UID: `auditctl -a always,exit -F arch=b64 -S execve -F uid=`. For unauthenticated access detection (CVE-2026-25089), search authentication logs for HTTP 200 responses to `/api/` or `/admin/` endpoints with no preceding successful login event for the source IP.

Evidence: This is an analysis step that reads but does not alter live state; however, before enabling verbose logging (which modifies appliance configuration), snapshot the current logging configuration (`show log setting` via FortiSandbox CLI) to preserve the pre-incident baseline. Key artifacts to analyze: (1) FortiSandbox web server access logs for HTTP requests to management API endpoints with injected characters or traversal sequences tied to CVE-2026-39808 and CVE-2026-39813; (2) FortiSandbox authentication audit logs for sessions that accessed administrative functions without a corresponding login event, consistent with the authentication bypass in CVE-2026-25089; (3) OS-level process creation logs (auditd or Sysmon Event ID 1) showing child processes spawned by the FortiSandbox web service — a shell process (sh, bash, cmd.exe) parented by the web daemon is a high-confidence indicator of successful CVE-2026-39808 exploitation; (4) Outbound network connections from the FortiSandbox host (netflow or firewall egress logs) that postdate the earliest anomalous HTTP request, which may indicate C2 establishment following RCE.

Step 3: Eradication — Apply Fortinet's official patches for CVE-2026-39813, CVE-2026-39808, and CVE-2026-25089 as published in the Fortinet PSIRT advisory (https://www.fortiguard.com/psirt — retrieve the specific advisory for these CVEs and confirm affected version ranges before patching). If patches are not yet available for your version, implement vendor-recommended workarounds. Reference: NIST SI-2 (Flaw Remediation); CIS 7.4 (Perform Automated Application Patch Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: If the Fortinet patch is not immediately available for your exact FortiSandbox version, implement the following manual workarounds: (1) Disable the FortiSandbox management web interface entirely and administer only via serial console or out-of-band SSH from a hardened jump host; (2) Apply a reverse proxy (nginx or HAProxy, free) in front of the management interface configured to block requests containing path traversal sequences (`..%2F`, `%2e%2e`, `../`) and shell metacharacters in query parameters — this partially mitigates CVE-2026-39808 and CVE-2026-39813 at the perimeter without touching the appliance firmware. Document the workaround as a formal exception with a defined remediation deadline per CIS 7.2.

Evidence: Before applying any Fortinet patch or firmware update, capture a full forensic image or at minimum a volatile state snapshot of the potentially compromised FortiSandbox: (1) Acquire a memory dump if the appliance OS supports it (FortiOS-based appliances may support `exec dump memory` — confirm with Fortinet support); (2) Export all current FortiSandbox job logs, submission history, and verdict records, as patching may alter or reset appliance state and these records document what malware analysis was conducted (or bypassed) during the compromise window; (3) Record the exact running firmware version (`get system status` via CLI) and all currently installed FortiSandbox components before patching alters the version table — this is required to confirm the advisory's affected version range applies and to document the pre-patch state for any subsequent forensic timeline; (4) Export the FortiSandbox configuration backup pre-patch. Patching the appliance will alter live state and these records cannot be recovered afterward.

Step 4: Recovery — After patching, rotate all FortiSandbox administrative credentials and API keys, as authentication bypass (CVE-2026-25089) may have permitted unauthorized access prior to remediation. Verify patch application against the Fortinet advisory version table. Monitor FortiSandbox for anomalous process execution and unexpected outbound connections for a minimum of 14 days post-remediation. Reference: D3-CRO (Credential Rotation); NIST AU-6 (Audit Record Review, Analysis, and Reporting).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AC-2 (Account Management), NIST AC-12 (Session Termination), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without PAM tooling, credential rotation of FortiSandbox admin accounts is performed via CLI: `config system admin; edit ; set password ; end`. Enumerate all API keys via `config system api-user` and delete or regenerate each. To monitor for post-patch persistence or re-exploitation without EDR, configure a cron job or scheduled task to run every 15 minutes: `ps aux | grep -E '(sh|bash|python|perl|nc|ncat)' | grep -v 'grep' >> /var/log/fortiSandbox/process_watch.log` — review this log daily for web-service-parented shells that would indicate CVE-2026-39808 re-exploitation. Monitor outbound DNS and HTTP from the FortiSandbox host using tcpdump: `tcpdump -i any -w /tmp/fsb_egress.pcap 'not host '` and rotate captures daily for 14 days.

Evidence: Before rotating credentials and revoking API keys (which alters live authentication state), export the complete current admin account inventory from FortiSandbox (`config system admin; show` via CLI) and document all active API user tokens (`config system api-user; show`). This preserves the pre-rotation account state needed to determine whether unauthorized admin accounts were created by an attacker exploiting CVE-2026-25089 — a persistence technique that credential rotation alone will not detect if the rogue account is not first identified and removed. Capture and retain the FortiSandbox audit log entries covering the authentication bypass window before any session termination action flushes active session state. Cross-reference newly discovered admin accounts against your CIS 5.1 account inventory baseline; any account not in that baseline is a high-confidence indicator of attacker persistence.

Step 5: Post-Incident — Conduct a review of patch management SLAs for critical security infrastructure. CVE-2026-25089 demonstrates that threat actors may possess pre-patch knowledge, requiring patch

application windows measured in hours, not days, for critical security tooling. Implement compensating controls per NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) to limit blast radius if a security appliance is compromised. Evaluate whether FortiSandbox management interfaces were exposed to the internet and remediate that exposure regardless of patch status.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: For teams without a vulnerability management platform, establish a manual SLA tracking process specifically for security infrastructure (FortiSandbox, SIEM, firewalls, EDR consoles): create a shared spreadsheet with columns for Asset, CVE, CVSS, Exploitation Status, Patch Available Date, and Patch Applied Date. Set a calendar alert to check the Fortinet PSIRT RSS feed (`https://www.fortiguard.com/rss/psirt.xml`) daily — this is free and requires no tooling. For CIS 5.4 enforcement on FortiSandbox without an enterprise PAM tool, create a dedicated admin-only account used exclusively for FortiSandbox administration and disable all other admin accounts from having management GUI access, enforced via `config system admin; set accprofile ` for non-admin users.

Evidence: This post-incident review phase does not alter live system state; however, the lessons-learned process should incorporate the forensic artifacts collected during previous phases as primary evidence. Specifically: (1) Retain the pre-patch web server access logs showing the full timeline of exploitation attempts against CVE-2026-39813, CVE-2026-39808, and CVE-2026-25089 — these provide the ground truth for measuring dwell time between public disclosure and exploitation onset, which directly informs the revised patch SLA; (2) Document whether internet exposure of the FortiSandbox management interface was recorded in the asset inventory (CIS 1.1) prior to this incident — a gap here indicates a configuration management failure separate from the vulnerability itself; (3) If a rogue admin account was discovered during credential rotation in Step 4, preserve that account's creation timestamp and associated session logs as evidence of the attacker's post-exploitation persistence TTPs for threat intelligence purposes.

Detection Guidance

Focus detection efforts on three behavioral patterns corresponding to the three CVEs. For CVE-2026-39813 (path traversal, CWE-22): search web access logs for HTTP requests containing encoded or raw path traversal sequences ('../', '%2e%2e%2f', '%252e') targeting FortiSandbox endpoints. For CVE-2026-39808 (OS command injection, CWE-78): look for web server processes (e.g., Apache, nginx, or FortiSandbox-specific daemons) spawning unexpected child processes such as shells (sh, bash, cmd.exe) or network utilities (curl, wget, nc). Alert on any command execution originating from the FortiSandbox web process context. For CVE-2026-25089 (missing authentication, CWE-306): identify HTTP requests successfully accessing authenticated administrative endpoints without a valid session token or with anomalous session identifiers. In SIEM, correlate: (1) source IPs sending requests to FortiSandbox management ports that have no prior authenticated session history; (2) HTTP 200 responses to administrative API paths from unauthenticated sources; (3) new administrative account creation or privilege changes on FortiSandbox following any of the above. No publicly shared IOCs (malicious hashes, attacker IPs, C2 domains) have been released in available source material as of this writing. Consult threat intelligence feeds and CISA advisories for updated IOCs as investigations proceed. D3FEND countermeasures applicable: D3-SFA (System File Analysis) to detect modification of FortiSandbox configuration files post-exploitation; D3-LAM (Local Account Monitoring) to detect unauthorized account creation.

Framework Mappings

MITRE-ATTACK

- **T1562.001** — Disable or Modify Tools
- **T1078.001** — Default Accounts
- **T1133** — External Remote Services
- **T1059** — Command and Scripting Interpreter
- **T1190** — Exploit Public-Facing Application
- **T1203** — Exploitation for Client Execution

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
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **AC-3** — Access Enforcement
- **SI-10** — Information Input Validation
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A03:2021** — Injection
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **16.12** — Implement Code-Level Security Checks
- **2.5** — Allowlist Authorized Software
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1562.001	Disable or Modify Tools	Defense-Evasion
T1078.001	Default Accounts	Defense-Evasion
T1133	External Remote Services	Persistence
T1059	Command and Scripting Interpreter	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1203	Exploitation for Client Execution	Execution

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/attackers-exploit-three-fortinet....	T3
Attackers are exploiting FortiSandbox vulnerabilities	https://www.helpnetsecurity.com/2026/06/16/fortisandbox-vulnerabili...	T3
Attackers Exploit Three Fortinet FortiSandbox Flaws, One Patched ...	https://thehackernews.com/2026/06/attackers-exploit-three-fortinet....	T3
CVE-2026-39813 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2026-39813	T1
CVE-2026-39808 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-39808	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-39813, CVE-2026-39808, CV...	T1

Generated 2026-06-16 19:20 UTC by TJS Security Command Center