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

Fortinet FortiSandbox Path Traversal Vulnerability Enables Privilege Escalation (CVE-2026-39813)

CVE VULNERABILITY | **HIGH** | CVSS 8.1 | **CISA KEV**

SCC Item ID	SCC-CVE-2026-0311
Type	CVE Vulnerability
CVE ID	CVE-2026-39813
Severity	HIGH
CVSS Base Score	8.1
EPSS Score	0.2364 (98th percentile)
KEV Status	Yes — CISA Known Exploited Vulnerability
Affected Products	Fortinet FortiSandbox 5.0.0 through 5.0.5; Fortinet FortiSandbox 4.4.0 through 4.4.8
Published	2026-06-15T00:00:00Z
Discovery Source	Vulncheck Kev

Executive Summary

A high-severity path traversal vulnerability in Fortinet FortiSandbox (CVE-2026-39813) allows attackers to escalate privileges by manipulating directory paths, with confirmed active exploitation recorded in both CISA and VulnCheck Known Exploited Vulnerability catalogs. Affected versions span FortiSandbox 4.4.0 through 4.4.8 and 5.0.0 through 5.0.5. Organizations running these versions face immediate risk of privilege escalation within their malware analysis infrastructure, which could undermine the integrity of the security controls FortiSandbox is designed to enforce.

Technical Analysis

CVE-2026-39813 is a path traversal vulnerability classified under CWE-24 (Path Traversal '../filedir') affecting Fortinet FortiSandbox versions 4.4.0-4.4.8 and 5.0.0-5.0.5. The flaw permits attackers to traverse directory structures using '../filedir' sequences, enabling privilege escalation on affected systems. Critically, exploitation may be possible by both authenticated and unauthenticated attackers, significantly broadening the attack surface. CVSS base score is 8.1 (High). EPSS score is 0.236 at the 97.5th percentile, indicating a very high likelihood of exploitation relative to all scored vulnerabilities. The vulnerability is confirmed actively exploited, appearing in both CISA KEV and VulnCheck KEV. MITRE ATT&CK techniques mapped include T1548 (Abuse

Elevation Control Mechanism) and T1083 (File and Directory Discovery). The originating advisory is Fortinet PSIRT FG-IR-26-112. CVSS vector is pending NVD publication. Patches should be sourced from the Fortinet PSIRT advisory at fortiguard.fortinet.com/psirt/FG-IR-26-112.

Action Checklist

1. Step 1: Containment, Immediately identify all FortiSandbox instances running versions 4.4.0-4.4.8 or 5.0.0-5.0.5 across your environment. Isolate internet-facing FortiSandbox management interfaces from public access using firewall rules or ACLs until patching is complete. Reference Fortinet PSIRT FG-IR-26-112 for Fortinet-specific network segmentation guidance (NIST AC-4: Information Flow Enforcement).
2. Step 2: Detection, Review FortiSandbox system and access logs for anomalous directory traversal patterns containing '../' sequences in file path parameters. Query web application and API gateway logs for requests with encoded traversal strings ('%2e%2e%2f', '..%2f', '../'). Check for unexpected privilege changes or process execution under elevated accounts following access to FortiSandbox endpoints. Correlate against T1548 and T1083 ATT&CK technique indicators (NIST AU-6: Audit Record Review, Analysis, and Reporting; CIS 8.2: Collect Audit Logs).
3. Step 3: Eradication, Apply the patched FortiSandbox versions identified in Fortinet PSIRT advisory FG-IR-26-112. Upgrade 4.4.x instances beyond 4.4.8 and 5.0.x instances beyond 5.0.5 per the advisory's specified remediation path. After patching, rotate credentials for all accounts that had access to affected FortiSandbox instances, as privilege escalation may have enabled credential access (D3-CRO: Credential Rotation; NIST AC-2: Account Management).
4. Step 4: Recovery, After patching, verify the FortiSandbox version string on each upgraded instance matches the fixed release listed in FG-IR-26-112. Re-enable management interface access incrementally, starting with internal-only access, and monitor AU logs for any recurrence of traversal patterns. Validate that no unauthorized accounts or scheduled tasks were created during the exposure window (NIST AU-6; D3-LAM: Local Account Monitoring).
5. Step 5: Post-Incident, Review whether FortiSandbox management interfaces were unnecessarily exposed to the internet or broad internal networks, and apply least-privilege network segmentation going forward. Assess whether existing vulnerability management processes would have caught this KEV-listed CVE faster; if not, adjust scanning scope to include security appliance management planes. Document control gaps against NIST AC-6 (Least Privilege) and CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/compliance immediately if forensic analysis confirms successful privilege escalation on any FortiSandbox instance — particularly if the compromised appliance processed or stored malware samples, network traffic captures, or file submissions containing customer data, as this may trigger breach notification obligations under GDPR, CCPA, or sector-specific regulations.

Recovery Notes	After patching all FortiSandbox instances to the fixed release per FG-IR-26-112, maintain enhanced monitoring of FortiSandbox authentication logs and web/API access logs for a minimum of 72 hours post-recovery, specifically hunting for recurrence of path traversal patterns ('../', '%2e%2e%2f') and any account activity from IPs identified during the incident. Verify the integrity of malware analysis results produced by FortiSandbox during the exposure window (versions 4.4.0–4.4.8 or 5.0.0–5.0.5), as a compromised sandboxing appliance may have produced manipulated or suppressed verdicts that affected downstream security decisions. Re-enable internet-facing management access only after confirming patched version strings, clean account audits, and no anomalous log activity for the full 72-hour monitoring window.
Forensic Artifacts	FortiSandbox web/API access logs at '/var/log/fortisandbox/' containing raw HTTP requests with path parameters — search for '../', '%2e%2e%2f', '..%2f', and '..%252f' double-encoded variants targeting FortiSandbox file-handling API endpoints, which would indicate active exploitation of the CVE-2026-39813 path traversal mechanism | Authentication and privilege escalation logs ('/var/log/fortisandbox/auth.log' or equivalent) showing account UID/GID transitions or sudo invocations by the FortiSandbox web service process immediately following traversal requests — evidence of successful privilege escalation post-traversal | Filesystem modification timestamps on sensitive directories accessible via path traversal (e.g., '/etc/', '/root/', FortiSandbox configuration directories) — files modified within the exploitation window with timestamps correlating to suspicious HTTP requests indicate attacker write access gained through the traversal | Cron jobs, systemd timers, and init scripts added or modified during the exposure window — path traversal with privilege escalation on FortiSandbox would enable an attacker to plant persistence mechanisms in standard Linux persistence locations accessible after privilege escalation to root | Network connection records (netflow or 'netstat'/'ss' snapshots) showing outbound connections from the FortiSandbox host to external IPs initiated by the web service or root processes during the exposure window — FortiSandbox's role as a sandboxing appliance with internet access makes it a viable pivot point for C2 egress following privilege escalation

Per-Action IR Details

Step 1: Containment — Immediately identify all FortiSandbox instances running versions 4.4.0–4.4.8 or 5.0.0–5.0.5 across your environment. Isolate internet-facing FortiSandbox management interfaces from public access using firewall rules or ACLs until patching is complete. Reference Fortinet PSIRT FG-IR-26-112 for Fortinet-specific network segmentation guidance (NIST AC-4: Information Flow Enforcement).

NIST Phase: Containment

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

Controls: 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: Run 'fortictl get system status | grep Version' on each FortiSandbox CLI to confirm version strings for 4.4.0–4.4.8 and 5.0.0–5.0.5. Block TCP/443 and TCP/80 to FortiSandbox management IPs at the perimeter firewall using an explicit deny ACL; use 'iptables -I INPUT -s 0.0.0.0/0 -d -p tcp --dport 443 -j DROP' on any Linux-based upstream gateway as an emergency measure until firewall rules are formalized.

Evidence: Before isolating the management interface, capture active TCP session state from the FortiSandbox host: run 'netstat -ano' or 'ss -tunap' to record all established connections to management ports (TCP/443, TCP/80, TCP/22). Export FortiSandbox system logs ('/var/log/fortisandbox/' and syslog forwarding buffer) and capture the running process list ('ps aux' or 'top -bn1') to preserve pre-isolation state. Document all source IPs connected to the management interface at the moment of isolation — these are candidate attacker IPs for path traversal exploitation.

Step 2: Detection — Review FortiSandbox system and access logs for anomalous directory traversal patterns containing '../' sequences in file path parameters. Query web application and API gateway logs for requests with encoded traversal strings ('%2e%2e%2f', '..%2f', '../'). Check for unexpected privilege changes or process execution under elevated accounts following access to FortiSandbox endpoints. Correlate against T1548 and T1083 ATT&CK technique indicators (NIST AU-6: Audit Record Review, Analysis, and Reporting; CIS 8.2: Collect Audit Logs).

NIST Phase: Detection Analysis

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

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

Compensating: Use 'grep' or 'zgrep' against FortiSandbox access logs to find traversal patterns: 'grep -iE "(\.\./|%2e%2e%2f|%2e%2e/|\.\./|\.\.%2f)" /var/log/fortisandbox/access.log'. Pipe output through 'awk' to extract timestamp, source IP, and URI. For privilege escalation evidence, search auth logs: 'grep -E "(sudo|su |FAILED|privilege|escalat)" /var/log/fortisandbox/auth.log'. Deploy a Sigma rule matching path traversal patterns in web server access logs targeting FortiSandbox API endpoints if log ingestion into a SIEM is available.

Evidence: This step is analytical and does not alter live system state, so no pre-action volatile capture is strictly required. However, before any remediation actions that follow, preserve: (1) FortiSandbox web/API access logs at '/var/log/fortisandbox/' showing raw HTTP requests with path parameters; (2) authentication and privilege escalation logs showing account changes or sudo usage post-traversal request; (3) a snapshot of '/etc/passwd' and '/etc/shadow' (or FortiSandbox user DB equivalent) to baseline account state before credential rotation; (4) process execution history showing any child processes spawned by the FortiSandbox web service under elevated UID/GID following exploitation.

Step 3: Eradication — Apply the patched FortiSandbox versions identified in Fortinet PSIRT advisory FG-IR-26-112. Upgrade 4.4.x instances beyond 4.4.8 and 5.0.x instances beyond 5.0.5 per the advisory's specified remediation path. After patching, rotate credentials for all accounts that had access to affected FortiSandbox instances, as privilege escalation may have enabled credential access (D3-CRO: Credential Rotation; NIST AC-2: Account Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.2 (Use Unique Passwords), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For teams without automated patch orchestration, download the fixed FortiSandbox firmware directly from Fortinet Support (support.fortinet.com) after verifying the SHA-256 checksum against FG-IR-26-112's published hash. Stage the upgrade during a maintenance window with a rollback snapshot if the hypervisor supports it. For credential rotation without a PAM tool, enumerate all local and LDAP-integrated accounts via 'fortictl get system admin' and issue forced password resets; document each rotation with a timestamp in the incident ticket.

Evidence: Before applying the patch or rotating credentials, capture: (1) full RAM dump of the FortiSandbox instance using a hypervisor-level memory snapshot (if virtualized) or 'dd' against '/dev/mem' to preserve any in-memory artifacts of privilege escalation or injected code; (2) a complete listing of all scheduled tasks and cron jobs ('crontab -l -u root', 'ls -la /etc/cron.*') to detect persistence mechanisms planted via the traversal before they are overwritten by the upgrade; (3) a copy of the FortiSandbox configuration export ('fortictl backup config') to compare pre- and post-patch configurations for unauthorized changes; (4) network connection state ('ss -tunap') immediately before patch application to record any active C2 or lateral movement sessions.

Step 4: Recovery — After patching, verify the FortiSandbox version string on each upgraded instance matches the fixed release listed in FG-IR-26-112. Re-enable management interface access incrementally, starting with internal-only access, and monitor AU logs for any recurrence of traversal patterns. Validate that no unauthorized accounts or scheduled tasks were created during the exposure window (NIST AU-6; D3-LAM: Local Account Monitoring).

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), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

Compensating: Verify patched version via FortiSandbox CLI: 'forticti get system status' and confirm the build number matches the FG-IR-26-112 fixed release. For account validation without an EDR, diff the current '/etc/passwd' and scheduled task outputs against the pre-patch baseline captured in Step 3 using 'diff baseline_passwd.txt <(cat /etc/passwd)'. Set up a cron-based integrity check: 'crontab -e' with a job that runs 'md5sum /etc/passwd /etc/cron.*' every 15 minutes and emails the hash delta to the security team during the 72-hour post-recovery monitoring window.

Evidence: Before re-enabling management interface access, verify there are no residual unauthorized processes running as root or the FortiSandbox service account by comparing 'ps aux' output against the pre-incident process baseline. Confirm no new cron jobs, systemd timers, or init scripts were added during the exposure window by checking modification timestamps: 'find /etc/cron* /etc/systemd/system -newer -ls'. These checks must be completed before restoring inbound management access to ensure attacker-planted persistence is not reactivated.

Step 5: Post-Incident — Review whether FortiSandbox management interfaces were unnecessarily exposed to the internet or broad internal networks, and apply least-privilege network segmentation going forward. Assess whether existing vulnerability management processes would have caught this KEV-listed CVE faster; if not, adjust scanning scope to include security appliance management planes. Document control gaps against NIST AC-6 (Least Privilege) and CIS 7.1 (Establish and Maintain a Vulnerability Management Process).

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AC-4 (Information Flow Enforcement), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Conduct a manual network exposure review by querying firewall rule sets with 'iptables -L -n -v' or reviewing NGF policy exports to identify any rules permitting inbound access to FortiSandbox management ports (TCP/443, TCP/22) from non-management subnets. Cross-reference against your asset inventory to confirm FortiSandbox appliances are included in vulnerability scanner scope (check scan targets in OpenVAS or Nessus Essentials configurations). Document findings in the lessons-learned report with specific rule IDs and scanner configuration changes needed.

Evidence: This post-incident review step does not alter live system state, so no pre-action volatile capture is required. For the lessons-learned record, preserve: (1) firewall rule exports showing the pre-incident management interface exposure configuration; (2) vulnerability scanner scope configuration showing whether FortiSandbox management IPs were included or excluded at the time CVE-2026-39813 was added to CISA KEV; (3) the incident timeline reconstructed from FortiSandbox access logs showing the earliest evidence of traversal attempts versus the date FG-IR-26-112 was published, to measure detection-to-response gap.

Detection Guidance

Search FortiSandbox access and application logs for HTTP or API requests containing directory traversal sequences: '../', '..%2f', '%2e%2e/', or URL-encoded equivalents in file path parameters. Alert on any successful responses (HTTP 200) to requests containing these patterns. Monitor for unexpected privilege escalation events in OS-level logs on the FortiSandbox host, including sudo usage or process execution under root by non-root accounts. Cross-reference with T1083 (File and Directory Discovery) by looking for enumeration of system directories outside expected sandbox submission paths. For network-based detection, deploy IPS signatures targeting path traversal attempts against FortiSandbox management ports. Relevant controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (Information System Monitoring), CIS 8.2 (Collect Audit Logs), D3-SFA (System File Analysis).

Framework Mappings

MITRE-ATTACK

- **T1548** — Abuse Elevation Control Mechanism
- **T1083** — File and Directory Discovery

NIST-800-53R5

- **AC-6** — Least Privilege
- **CM-6** — Configuration Settings
- **IR-5** — Incident Monitoring

ISO-27001-2022

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

NIST-CSF-2

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

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

SOC2-TSC

- **CC6.3** — Authorizes, modifies, or removes access

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1083	File and Directory Discovery	Discovery

Sources

Source	URL	Tier
vulncheck_kev	https://nvd.nist.gov/vuln/detail/CVE-2026-39813	T1
CVE-2026-39813 Detail - NVD	https://nvd.nist.gov/vuln/detail/cve-2026-39813	T1
Fortinet PSIRT FG-IR-26-112 - FortiGuard Labs	https://fortiguard.fortinet.com/psirt/FG-IR-26-112	T3

Source	URL	Tier
CVE-2026-39813 - Exploits & Severity - Feedly	https://feedly.com/cve/CVE-2026-39813	T3
CVE-2026-39813: FortiSandbox Path Traversal Vulnerability	https://www.sentinelone.com/vulnerability-database/cve-2026-39813/	T3
CISA KEV	https://www.cisa.gov/known-exploited-vulnerabilities-catalog	T1

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