NCA-13.180626 – National CERT Advisory

Critical Vulnerabilities in Fortinet FortiSandbox Under Active Exploitation (CVE-2026-39808, CVE-2026-39813, CVE-2026-25089)

National CERT Pakistan has assessed an elevated cyber risk posture following confirmed active exploitation attempts targeting multiple critical vulnerabilities in Fortinet FortiSandbox deployments, including FortiSandbox Cloud and FortiSandbox PaaS environments.

These vulnerabilities may allow unauthenticated remote attackers to execute arbitrary operating system commands and bypass authentication mechanisms, resulting in full compromise of affected sandbox security infrastructure. Security researchers have observed active scanning and exploitation attempts against internet-exposed FortiSandbox instances.

Organizations that have not applied vendor-issued security updates remain at high risk of compromise.

DOCUMENT SUMMARY

Field	Details
Advisory ID	NCA-13.180626
Threat Type	OS Command Injection, Authentication / Access Control Weakness, Remote Code Execution Risk
Severity	Critical (Active Exploitation Observed)
Attack Vector	Remote network exploitation against FortiSandbox Web UI and JRPC API
Authentication Required	None
User Interaction	Not Required
CVSS Score	Up to 9.8 (CVE-2026-25089)
Scope & Applicability	Government, CII, financial institutions, enterprises using FortiSandbox
Affected Products	FortiSandbox, FortiSandbox Cloud, FortiSandbox PaaS
Security Advisory Source	Fortinet PSIRT advisories

IMPACT ANALYSIS

Failure to remediate these vulnerabilities may result in:

1. Remote unauthenticated command execution on FortiSandbox appliances
2. Complete system compromise of sandbox analysis infrastructure
3. Unauthorized administrative access via authentication bypass
4. Deployment of malware through compromised security systems
5. Credential harvesting and sensitive data exposure
6. Lateral movement into enterprise networks
7. Establishment of persistent footholds within security infrastructure
8. Manipulation or disabling of security inspection workflows
9. Potential disruption of enterprise threat analysis capabilities
10. Broader compromise of interconnected organizational environments

THREAT CHARACTERISTICS

Characteristic	Details
Threat Category	Exploited Security Appliance Vulnerability
Threat Status	Active exploitation attempts observed

Root Cause	OS Command Injection & Authentication Bypass flaws
Attack Surface	Internet-facing FortiSandbox Web UI / API
Attack Complexity	Low (remote exploitation feasible)
Privileges Required	None
Impact Scope	Full system compromise
CWE Classes	CWE-78 (OS Command Injection), CWE-306 (Missing Authentication), CWE-287 (Improper Authentication)

VULNERABILITY DETAILS

- **CVE-2026-39808** – Critical FortiSandbox flaw associated with unauthenticated remote exploitation and command execution
- **CVE-2026-39813** – Authentication or access-control-related flaw
- **CVE-2026-25089** – OS command injection vulnerability that may allow unauthenticated remote attackers to execute arbitrary commands on affected systems

INDICATORS OF EXPOSURE / TARGETING (IoEs)

No fixed global IoC set has been confirmed at this stage. Organizations should actively hunt for the following indicators within FortiSandbox logs and telemetry:

1. Suspicious Activity Patterns

- Repeated unauthorized access attempts to Web UI or API endpoints
- Unexpected administrative session creation
- Unauthenticated API requests to JRPC interfaces
- Abnormal command execution logs in sandbox environment

2. Exploitation Behavior Indicators

- Command execution events originating from external IPs
- Authentication logs missing corresponding session validation
- Unexpected process spawning from web service context
- Sandbox system spawning shell or system utilities

3. Network Indicators

- Unusual inbound traffic to FortiSandbox management interfaces
- Repeated scanning of exposed appliance endpoints
- High-frequency automated requests to API endpoints

REMEDIATION ACTIONS

1. Immediate Defensive Controls

Action Category	Recommended Actions
Patch Management	Apply the latest Fortinet security updates immediately to all affected FortiSandbox deployments, including cloud and PaaS instances.
Exposure Control	Remove FortiSandbox administrative and management interfaces from direct public internet exposure and restrict access through trusted networks only.

Access Restriction	Limit Web UI, API, and JRPC access to approved internal hosts, VPN gateways, or dedicated management segments.
MFA Enforcement	Enable MFA for all administrative access paths and review exceptions or legacy accounts.
Log Review	Review authentication, API, process execution, and administrative activity logs for signs of exploitation or anomalous behavior.
Threat Hunting	Hunt for suspicious command execution, unauthorized session creation, external scanning activity, and abnormal process spawning from web-service context.
Incident Containment	Isolate potentially compromised appliances immediately and preserve logs for forensic review.
Credential Security	Rotate administrative credentials after patching and after any indication of suspicious access.
Service Hardening	Disable unused APIs, interfaces, and external administrative access paths wherever operationally feasible.
Session Monitoring	Terminate suspicious or unknown sessions

2. Enhanced Monitoring & Detection

- Enable detailed FortiSandbox logging and audit trails
- Monitor Web UI and API authentication anomalies
- Deploy SIEM rules for command injection patterns
- Correlate firewall logs with sandbox activity logs
- Detect unexpected process execution spawned by web services
- Implement behavioral anomaly detection for admin actions

3. Incident Response Requirements

Organizations must:

- Investigate all internet-facing FortiSandbox systems
- Review authentication and command execution logs
- Isolate potentially compromised appliances immediately
- Conduct credential rotation for administrative accounts
- Preserve logs for forensic investigation
- Validate system integrity and configuration baselines

ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps	Priority
Patch Deployment	Apply Fortinet security updates	**CRITICAL**
Exposure Reduction	Remove public-facing admin interfaces	**CRITICAL**
Threat Hunting	Search for command injection indicators	**CRITICAL**
Log Review	Analyze authentication and API logs	**HIGH**
Credential Reset	Rotate admin credentials	**HIGH**
Incident Escalation	Report suspected compromise	**HIGH**

MONITORING & DETECTION REQUIREMENTS

1. Monitor unauthorized administrative access attempts
2. Detect abnormal API or JRPC request patterns
3. Identify command execution anomalies
4. Track missing authentication validation events

5. Monitor unexpected process spawning
6. Detect external scanning of FortiSandbox interfaces
7. Validate integrity of sandbox execution environment
8. Correlate firewall and appliance logs
9. Monitor lateral movement from sandbox systems
10. Detect anomalous outbound connections from appliances

INCIDENT REPORTING

All suspected compromise, exploitation attempts, or anomalous activity must be immediately reported to National CERT Pakistan:

- **Incident Reporting Portal:** https://pkcert.gov.pk/report-incident/
- **Email:** cert@pkcert.gov.pk
- **UAN:** +92 519203412

CALL TO ACTION – KEY IMPERATIVES

#	Requirement
1	Apply Fortinet security patches immediately
2	Remove internet exposure of FortiSandbox systems
3	Monitor authentication and API logs continuously
4	Investigate indicators of command injection activity
5	Enforce MFA for administrative access
6	Conduct compromise assessment of all appliances
7	Escalate confirmed incidents to National CERT
8	Strengthen perimeter security controls

ADVISORY NOTE: Organizations operating FortiSandbox infrastructure are strongly advised to treat this as an active exploitation scenario. Immediate remediation, continuous monitoring, and proactive threat hunting are essential to prevent unauthorized access and potential compromise of enterprise security analysis environments.