NCA-03.190126 – National CERT Advisory – Critical Fortinet FortiSIEM and FortiOS Remote Code Execution Vulnerabilities

INTRODUCTION

Fortinet has disclosed multiple critical vulnerabilities affecting FortiSIEM, FortiOS, FortiSwitchManager, and FortiFone products. The most severe of these is CVE-2025-64155, affecting FortiSIEM with a CVSS score of 9.4, which allows unauthenticated remote attackers to execute arbitrary code and take complete control of affected systems.

The vulnerability stems from flaws in FortiSIEM management components that require no valid credentials for exploitation. Internet-facing deployments are especially vulnerable, with attackers able to gain full control of the appliance remotely over the network. The availability of a public proof-of-concept exploit significantly increases the risk of active exploitation.

Additional critical vulnerabilities have been disclosed including CVE-2025-25249 (affecting FortiOS and FortiSwitchManager) which allows arbitrary code execution via the cw_acd daemon, and CVE-2025-47855 (CVSS 9.3) affecting FortiFone devices. Together, these issues represent a broader wave of high-impact vulnerabilities across Fortinet products requiring immediate remediation.

CVSS Score: 9.4 (Critical)
Attack Vector: Network/Remote
Authentication Required: None
User Interaction: None

IMPACT

Unauthenticated Remote Code Execution, Full System Compromise, Security Monitoring Manipulation, Configuration Tampering, Detection Evasion, Lateral Movement

Successful exploitation may lead to:

1. **Remote Code Execution** – Complete ability to execute arbitrary system commands on FortiSIEM, FortiOS, and FortiFone systems
2. **Full System Compromise** – Total control over affected Fortinet appliances and underlying infrastructure
3. **Security Monitoring Manipulation** – Unauthorized ability to modify, disable, or delete security monitoring data and logs
4. **Configuration Tampering** – Unauthorized access to modify system configurations and security policies

5. **Detection Capability Disabling** – Ability to turn off or bypass security detection mechanisms
6. **Credential Theft** – Access to stored credentials, API keys, and authentication tokens
7. **Lateral Movement** – Potential to compromise additional systems within the enterprise network
8. **Data Exfiltration** – Exposure of sensitive security monitoring data and enterprise information
9. **Supply Chain Risk** – Compromised security infrastructure could affect entire organizational security posture

THREAT DETAILS

Vulnerability Overview

Primary Vulnerability:

- **Incident ID:** Fortinet Critical RCE – CVE-2025-64155
- **Affected Component:** Fortinet FortiSIEM management components
- **Vulnerability ID:** CVE-2025-64155
- **Description:** Critical remote code execution vulnerability that allows unauthenticated attackers to execute arbitrary code and take complete control of FortiSIEM systems

High severity (CVSS 7.4) heap buffer overflow via cw_acd daemon":

- **CVE-2025-25249:** Arbitrary code execution via the cw_acd daemon in FortiOS and FortiSwitchManager
- **CVE-2025-47855:** Critical vulnerability (CVSS 9.3) affecting FortiFone devices

Attack Characteristics

- **Attack Vector:** Network/Remote
- **Attack Complexity:** Low
- **Privileges Required:** None
- **User Interaction:** None
- **CVSS Score:** 9.4 (Critical)
- **Likely CWE:** CWE-20 (Improper Input Validation), CWE-862 (Missing Authorization)

Exploitation Requirements

Exploitation requires:

- A vulnerable version of FortiSIEM, FortiOS, FortiSwitchManager, or FortiFone
- Network accessibility to the affected Fortinet appliance
- No credentials or user interaction
- Exposed management components

The vulnerability is confirmed exploitable with a public proof-of-concept available, and organizations running vulnerable Fortinet products face immediate and severe risk of complete system compromise.

Context: Broader Fortinet Vulnerability Pattern

This disclosure represents a wave of high-impact vulnerabilities across multiple Fortinet product lines:

- **CVE-2025-64155** (CVSS 9.4) – FortiSIEM
- **CVE-2025-25249** – FortiOS and FortiSwitchManager
- **CVE-2025-47855** (CVSS 9.3) – FortiFone

This pattern indicates sustained attacker interest in Fortinet products and heightened risk for organizations using these security infrastructure components.

INDICATORS OF COMPROMISE (IoCs)

Category	Indicator / Value	Description / Notes	Action Required
Unauthorized Access Events	Unexpected administrative actions or API calls to FortiSIEM/FortiOS	Indicates possible RCE exploitation	Immediately review access logs and correlate source IPs
System Process Anomalies	Unusual process spawning, especially from cw_acd daemon or management services	Suggests arbitrary command execution	Investigate running processes and terminate suspicious activity
Configuration Changes	Unapproved configuration modifications or policy changes	Attacker-driven system tampering	Review configuration change history and restore from backups
File System Changes	Unauthorized file creation, modification, or deletion on appliances	Potential malware deployment or data theft	Conduct file integrity monitoring and forensic analysis
Network Indicators	Unrecognized IP addresses accessing management interfaces	May indicate malicious reconnaissance or exploitation	Block suspicious IPs and restrict network access
Service Behavior	Unexpected service restarts, crashes, or anomalous behavior	Possible exploitation attempts or post-compromise activity	Monitor service status and investigate anomalies
Credential Access	Unusual access to stored credentials or authentication systems	Possible credential harvesting	Rotate all credentials and review access patterns

Outbound Connections	Unexpected external connections or data transfers from appliances	Potential data exfiltration or C2 communication	Monitor network egress and block unauthorized connections
Log Tampering	Missing, modified, or cleared security logs	Attacker attempting to cover tracks	Enable remote log forwarding and investigate gaps
Detection Disabling	Security features or monitoring capabilities disabled unexpectedly	Attacker evading detection	Re-enable security features and investigate who/what disabled them

AFFECTED VERSIONS

Product	CVE	Affected Versions
FortiSIEM	CVE-2025-64155	7.4.0 7.3.0-7.3.4 7.1.0-7.1.8 7.0.0-7.0.4 6.7.0-6.7.10
FortiOS	CVE-2025-25249	7.6.0-7.6.3 7.4.0-7.4.8 7.2.0-7.2.11 7.0.0-7.0.17 6.4.0-6.4.16
FortiSwitchManager	CVE-2025-25249	7.2.0-7.2.6 7.0.0-7.0.5
FortiFone	CVE-2025-47855	Various versions by model

Note: Specific affected and fixed version details vary by product and release branch. Administrators should refer to Fortinet's official PSIRT advisories for the authoritative list of affected and fixed versions.

PATCHED VERSIONS

Patching Recommendations

1. **Apply the latest security patches released by Fortinet** for FortiSIEM, FortiOS, FortiSwitchManager, and FortiFone without delay
2. **Prioritize patching internet-facing and security-critical systems**, particularly FortiSIEM deployments exposed to untrusted networks
3. **Validate successful patch application** and restart affected services where required
4. **Rotate all credentials and authentication tokens** stored within or managed by affected systems after patching

5. **Review audit logs** for unauthorized changes, suspicious activity, or signs of exploitation
6. **Review Fortinet PSIRT advisories** to ensure all relevant fixes across product lines have been applied
7. **Test patches** in non-production environments before deploying to critical infrastructure where possible
8. Official Patch Details: https://fortiguard.com/psirt/FG-IR-25-772

Patching Summary

Version Category	Components / Modules	Status
Vulnerable	FortiSIEM versions 7.4.0, 7.3.0-7.3.4, 7.1.0-7.1.8, 7.0.0-7.0.4, 6.7.0-6.7.10	Must patch immediately
Vulnerable	FortiOS versions 7.6.0-7.6.3, 7.4.0-7.4.8, 7.2.0-7.2.11, 7.0.0-7.0.17, 6.4.0-6.4.16	Must patch immediately
Vulnerable	FortiSwitchManager versions 7.2.0-7.2.6, 7.0.0-7.0.5	Must patch immediately
Vulnerable	FortiFone (various versions)	Must patch immediately
Secure	Latest patched versions per Fortinet PSIRT advisories	Recommended - verify installation

RECOMMENDATIONS & MITIGATION ACTIONS

1. Patch Immediately (Recommended Fix)

- **Apply the latest security patches released by Fortinet** for all affected products without delay
- **Prioritize internet-facing systems** and security-critical FortiSIEM, FortiOS, and FortiFone deployments
- **Validate successful patch application** and restart affected services where required
- **Rotate all credentials, API keys, and authentication tokens** after patching
- **Review audit logs and security monitoring data** for any signs of unauthorized access or compromise
- **Conduct security assessment** of all affected systems for signs of exploitation
- **Verify patch effectiveness** through testing and validation before returning to production

2. Temporary Mitigation (If Immediate Patching Not Feasible)

CRITICAL: These mitigation steps reduce exposure but do NOT eliminate risk. Patching remains the only complete remediation.

- **Restrict network access to Fortinet appliances** using firewalls, VPNs, or allowlists

    - Implement IP allowlisting for administrative and management interfaces
    - Deploy network segmentation to isolate FortiSIEM, FortiOS, and other Fortinet systems
    - Use VPN or zero-trust network access for administrative access
    - Enforce strict access controls around management components

- **Disable public access to management interfaces** and untrusted network exposure

    - Place management interfaces behind reverse proxy with authentication
    - Disable unnecessary external-facing administrative endpoints
    - Restrict FortiSIEM access to trusted internal networks only

- **Monitor system logs and network for signs of exploitation activity**

    - Enable detailed logging for all administrative activities
    - Deploy intrusion detection/prevention systems
    - Set up alerts for suspicious command execution and process spawning
    - Monitor for unexpected service behavior or configuration changes

- **Consider temporarily isolating affected systems** until remediation is complete

    - Assess business impact of isolation vs. risk of exploitation
    - Migrate critical security monitoring to patched or alternative systems
    - Establish compensating controls for isolated systems

NOTE: These steps are not a replacement for patching. Mitigation steps reduce exposure but do not eliminate risk. Patching is the only way to achieve complete remediation.

3. Strengthen Security Posture

- **Implement least-privilege access controls** for all Fortinet appliance administrators and service accounts
- **Enable comprehensive audit logging** for all administrative actions and system activities
- **Deploy network monitoring and intrusion detection systems** around security infrastructure
- **Establish regular vulnerability assessment and patching schedules** for all Fortinet products
- **Implement secure credential management practices** using secrets vaults and rotation policies
- **Conduct security awareness training** for administrators of security infrastructure
- **Establish incident response procedures** for security infrastructure compromise scenarios
- **Implement defense-in-depth strategies** to protect critical security systems
- **Enable remote log forwarding** to prevent log tampering by attackers
- **Establish baseline behavior monitoring** for all Fortinet appliances

4. Action Summary & Response Priorities

The following table summarizes required actions, priorities, and recommended timeframes for responding to CVE-2025-64155 and related Fortinet vulnerabilities.

Action Type	Specific Steps	Priority	Timeframe
Patching (Fix)	- Apply latest Fortinet security patches for all affected products - Prioritize internet-facing and security-critical systems - Validate successful patch application and restart services - Rotate all credentials and authentication tokens - Review audit logs for signs of compromise - Test patches before deploying to production where possible	MANDATORY	Immediate (today)
Temporary Mitigation	- Restrict network access using firewalls, VPNs, or allowlists - Implement IP allowlisting for management interfaces - Disable public access to administrative interfaces - Place management behind reverse proxy with authentication - Isolate affected systems where possible - Enforce strict network segmentation	HIGH	Next 24–48 hours
Hardening (Ongoing)	- Enforce least-privilege access controls - Enable comprehensive audit logging - Deploy network monitoring and IDS/IPS - Use a secret vault for credential management - Perform regular vulnerability scanning - Establish and test incident response procedures - Enable remote log forwarding - Establish baseline behavior monitoring	REQUIRED	Continuous

MONITORING & DETECTION

Organizations should implement the following monitoring measures:

- **Monitor for unusual administrative activity** or unauthorized access to management interfaces
- **Alert on unexpected process spawning** or command execution, especially from cw_acd daemon or management services
- **Track configuration changes** and alert on unauthorized modifications to security policies
- **Deploy file integrity monitoring** on Fortinet appliance system directories
- **Monitor network traffic** for suspicious outbound connections from Fortinet appliances
- **Review audit logs** for unauthorized administrative actions or privilege escalations
- **Establish baseline behavior** for Fortinet appliance usage and alert on deviations
- **Implement SIEM correlation rules** for RCE exploitation indicators
- **Monitor for known exploit signatures** in network traffic targeting FortiSIEM and FortiOS
- **Track failed authentication attempts** and unusual access patterns to management interfaces
- **Monitor for security feature disabling** or unexpected service behavior
- **Alert on log tampering** or gaps in security monitoring data
- **Monitor for lateral movement** from compromised Fortinet appliances to other systems

REFERENCES

- https://fortiguard.fortinet.com/psirt/FG-IR-25-772
- https://nvd.nist.gov/vuln/detail/CVE-2025-64155
- https://secure-iss.com/soc-advisory-fortinet-fortisiem-fortios-critical-vulnerabilities-14-jan-2026/
- https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-fortinet-products-could-allow-for-arbitrary-code-execution-2026-003

CALL TO ACTION

The National CERT urges all organizations to:

1. **Immediately apply Fortinet security patches** for FortiSIEM, FortiOS, FortiSwitchManager, and FortiFone products
2. **Prioritize internet-facing and security-critical deployments** for immediate remediation
3. **Implement temporary mitigations** if immediate patching is not feasible
4. **Rotate all credentials and authentication tokens** stored within or managed by affected systems
5. **Conduct comprehensive log reviews** to detect any signs of exploitation or compromise
6. **Restrict network access** to Fortinet appliances using defense-in-depth approaches
7. **Establish continuous monitoring** for suspicious activity across all Fortinet infrastructure
8. **Ensure all Fortinet deployments** are inventoried, assessed, and secured

9. **Review Fortinet PSIRT advisories** regularly to stay informed of additional security updates

Immediate action is critical to prevent complete system compromise, security monitoring manipulation, detection evasion, and potential enterprise-wide breach enabled by these critical remote code execution vulnerabilities affecting core security infrastructure.