INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-12 14:09 UTC

FortiOS CAPWAP Daemon Out-of-Bounds Write Allows Code Execution via Compromised Managed Devices (CVE-2025-53844)

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0162
Type	CVE Vulnerability
CVE ID	CVE-2025-53844
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Fortinet FortiOS 7.6.0-7.6.3, 7.4.0-7.4.8, 7.2.0-7.2.11; attack vector devices: FortiAP, FortiExtender, FortiSwitch
Published	2026-05-12T07:00:00+00:00
Discovery Source	Rss:T1 Psirt

Executive Summary

A high-severity vulnerability in Fortinet FortiOS allows an attacker who has already compromised a managed edge device (FortiAP, FortiExtender, or FortiSwitch) to execute code on the FortiGate firewall itself. Affected versions span FortiOS 7.2.0 through 7.6.3, covering a wide range of enterprise deployments. Patches are available; organizations running affected versions with managed wireless or switching infrastructure should prioritize remediation within the next patch cycle or within 30 days, whichever is sooner, to prevent lateral movement from a perimeter device to core network security infrastructure.

Technical Analysis

CVE-2025-53844 is an out-of-bounds write (CWE-787) in the CAPWAP daemon of Fortinet FortiOS. Affected versions: 7.2.0-7.2.11, 7.4.0-7.4.8, 7.6.0-7.6.3. The attack vector is lateral: an attacker must first compromise an authenticated FortiAP, FortiExtender, or FortiSwitch device managed by the target FortiGate. From that position, the attacker can send malformed CAPWAP control messages to trigger the out-of-bounds write condition and achieve code execution on the FortiGate appliance. MITRE technique mapping includes T1210 (Exploitation of Remote Services), T1068 (Exploitation for Privilege Escalation), T1059 (Command and Scripting Interpreter), T1021 (Remote Services), T1548 (Abuse Elevation Control Mechanism), and T1190 (Exploit Public-Facing Application). CVSS base score is 7.5 (NVD); vendor reporting indicates 8.3. Treat as High severity pending

FortiGuard or NVD confirmation of the authoritative score. No active exploitation has been reported. No CISA KEV listing as of configuration date. Patches are available across all three affected branches per FortiGuard PSIRT advisory FG-IR-26-123 (https://fortiguard.fortinet.com/psirt/FG-IR-26-123).

Action Checklist

1. Step 1: Containment - Identify all FortiGate appliances running FortiOS 7.2.0-7.2.11, 7.4.0-7.4.8, or 7.6.0-7.6.3 in your environment. Audit which of those FortiGates have FortiAP, FortiExtender, or FortiSwitch devices managed via CAPWAP. Treat any compromised or unverified managed edge device as a potential attack source and isolate it from the FortiGate management plane pending patching.
2. Step 2: Detection - Review FortiGate logs for anomalous CAPWAP daemon activity, unexpected process crashes, or core dumps associated with the CAPWAP service. If you have a SIEM, query it for unusual traffic patterns between managed FortiAP/FortiExtender/FortiSwitch devices and the FortiGate control plane; otherwise, review FortiGate firewall logs directly for such patterns. Look for unauthorized commands or sessions originating from managed device IP addresses. Check FortiOS event logs for authentication anomalies on managed device accounts.
3. Step 3: Eradication - Apply the patches issued by Fortinet for the affected branches per FortiGuard PSIRT advisory FG-IR-26-123. Upgrade FortiOS to patched versions (minimum: 7.2.12, 7.4.9, or 7.6.4, confirm exact fixed versions in FortiGuard PSIRT FG-IR-26-123). Verify patch integrity against Fortinet's published checksums before deployment. Review and rotate credentials for all managed FortiAP, FortiExtender, and FortiSwitch devices.
4. Step 4: Recovery - After patching, confirm the CAPWAP daemon is running the updated binary. Validate managed device re-authentication and normal CAPWAP handshake behavior in FortiGate logs. Monitor for any residual anomalous activity from previously managed devices for at least 72 hours post-patch. Re-baseline normal CAPWAP traffic patterns in your SIEM or log analysis tool.
5. Step 5: Post-Incident - This vulnerability exposes a lateral movement path from managed edge devices to core firewall infrastructure. Review network segmentation between management plane traffic and production traffic. Evaluate whether managed device compromise detection (integrity monitoring, configuration drift alerts) is in place. Assess whether the principle of least privilege is enforced on FortiAP, FortiExtender, and FortiSwitch management accounts. Document findings for the next architecture review.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal counsel if forensic evidence — specifically cw_acd core dumps, unauthorized FortiGate admin sessions, or configuration changes not attributable to authorized staff — indicates the CAPWAP vulnerability was actively exploited and the FortiGate firewall itself was compromised, as this constitutes a breach of the network perimeter control with potential regulatory notification obligations if PII/PHI traverses the affected FortiGate.

Recovery Notes	After patching all affected FortiOS branches to fixed versions per FortiGuard FG-IR-26-123, verify the CAPWAP daemon (cw_acd) binary version and confirm clean CAPWAP handshake sequences for every re-onboarded FortiAP, FortiExtender, and FortiSwitch device before restoring them to production management. Monitor FortiGate crash logs and CAPWAP event logs continuously for 72 hours post-patch, treating any new cw_acd crash or unexpected managed-device tunnel request as an active incident indicator. Re-baseline CAPWAP control plane traffic volume and session counts in your SIEM or manual PCAP baseline immediately post-patch to enable anomaly detection against future exploitation attempts targeting this or related CAPWAP vulnerabilities.
Forensic Artifacts	Core dump files at /var/core/cw_acd.* on the FortiGate: the primary artifact of a successful or attempted out-of-bounds write exploit against the CAPWAP daemon, with crash timestamps correlatable to managed device activity. | FortiGate CAPWAP subsystem event logs (wireless-controller logid range 0104xxxx) showing tunnel state changes, malformed Join Request or Configuration Status Update messages, or authentication failures from specific FortiAP or FortiExtender serial numbers and IPs. | Raw PCAP of UDP 5246 (CAPWAP control) and UDP 5247 (CAPWAP data) traffic between managed device subnets and FortiGate management IP, inspected for CAPWAP element TLVs with anomalous length fields indicative of the out-of-bounds write payload delivery. | FortiGate administrative session logs showing any new CLI or GUI logins, configuration changes, or privilege escalations on the FortiGate itself occurring within the window of anomalous CAPWAP activity — direct evidence of post-exploitation activity if successful code execution occurred. | FortiOS running configuration snapshots (pre- and post-patch) exported via 'execute backup config', used to identify any unauthorized configuration modifications to firewall policies, admin accounts, or managed device profiles that a post-exploitation actor may have introduced through the compromised CAPWAP daemon.

Per-Action IR Details

Step 1: Containment — Identify all FortiGate appliances running FortiOS 7.2.0–7.2.11, 7.4.0–7.4.8, or 7.6.0–7.6.3 in your environment. Audit which of those FortiGates have FortiAP, FortiExtender, or FortiSwitch devices managed via CAPWAP. Treat any compromised or unverified managed edge device as a potential attack source and isolate it from the FortiGate management plane pending patching.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST CM-8 (System Component Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'get system status' and 'get system fortiguard-service status' via FortiOS CLI on each FortiGate to confirm running version. Use 'show wireless-controller wtp' and 'show switch-controller managed-switch' to enumerate all CAPWAP-managed FortiAP and FortiSwitch devices. To isolate suspect managed devices without full network downtime, disable the CAPWAP tunnel to individual FortiAP units via 'config wireless-controller wtp' → 'set admin disable' and apply an ACL on the FortiGate management interface to drop inbound CAPWAP (UDP 5246/5247) from unverified device IPs using: 'config firewall policy' with source restricted to known-good device addresses.

Evidence: Before isolating any managed device, capture: (1) FortiGate CAPWAP daemon process list snapshot via 'diag sys process list | grep capwap' to record PID and memory footprint at time of isolation; (2) FortiGate event log entries from /var/log/fortigate/eventlog showing CAPWAP tunnel establishment events for each managed device, including device serial numbers and source IPs; (3) Any existing core dump files in /var/core/ on the FortiGate, which would indicate prior CAPWAP daemon crashes potentially triggered by malformed out-of-bounds write payloads from a compromised managed device; (4) Full FortiSwitch/FortiAP configuration export via 'execute backup config' before any changes.

Step 2: Detection — Review FortiGate logs for anomalous CAPWAP daemon activity, unexpected process crashes, or core dumps associated with the CAPWAP service. Query SIEM for unusual traffic patterns between managed FortiAP/FortiExtender/FortiSwitch devices and the FortiGate control plane. Look for unauthorized commands or sessions originating from managed device IP addresses. Check FortiOS event logs for authentication anomalies on managed device accounts.

NIST Phase: Detection Analysis

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

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use the following targeted FortiOS CLI commands: (1) 'diag debug crashlog read' to retrieve crash logs specific to the CAPWAP daemon (cw_acd process); (2) 'diag log test' followed by reviewing /var/log/fortigate/ for event entries with logid matching CAPWAP subsystem events (logid range 0104 for wireless events); (3) Run 'diag sys session list | grep 5246' and 'diag sys session list | grep 5247' to enumerate all active CAPWAP control and data channel sessions and flag any from unexpected source IPs; (4) Use Wireshark or 'tcpdump -i any port 5246 or port 5247 -w capwap_capture.pcap' on a span port to capture raw CAPWAP control plane traffic and inspect for malformed CAPWAP element TLVs that would indicate exploit payload delivery; (5) Deploy a Sigma rule matching FortiGate syslog output for process name 'cw_acd' with signal 11 (SIGSEGV) or signal 6 (SIGABRT) to detect daemon crash indicative of triggered out-of-bounds write.

Evidence: Capture before analysis concludes: (1) FortiGate system event logs filtered for CAPWAP subsystem events — specifically log entries from the wireless-controller and cw_acd daemon showing tunnel state changes, authentication failures, or malformed message errors from managed FortiAP (serial numbers and IPs) or FortiExtender devices; (2) Core dump files at /var/core/cw_acd.* on the FortiGate, which are the primary forensic artifact of a successful or attempted out-of-bounds write exploit against the CAPWAP daemon; (3) NetFlow or raw PCAP of UDP 5246/5247 traffic between managed device subnets and FortiGate management IP, looking for CAPWAP Discovery Request or Join Request messages with anomalous element lengths; (4) FortiOS auth logs for any new administrative sessions or configuration changes on the FortiGate that occurred within the window of anomalous CAPWAP activity, which would suggest successful code execution and post-exploitation.

Step 3: Eradication — Apply the patches issued by Fortinet for the affected branches per FortiGuard PSIRT advisory FG-IR-26-123. Upgrade FortiOS to a version outside the affected ranges (above 7.2.11, 7.4.8, and 7.6.3 respectively, or the fixed versions specified in the FortiGuard advisory). Verify patch integrity against Fortinet's published checksums before deployment. Review and rotate credentials for all managed FortiAP, FortiExtender, and FortiSwitch devices.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IA-5 (Authenticator Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Before upgrading, verify FortiOS firmware image SHA-256 checksum against the value published in FortiGuard advisory FG-IR-26-123 using 'sha256sum ' on a Linux host or 'certutil -hashfile SHA256' on Windows — do not skip this step, as a compromised managed device could theoretically be used to stage a supply-chain intercept. Perform upgrade via FortiGate GUI (System → Firmware) or CLI ('execute restore image ftp '). For credential rotation on managed FortiAP and FortiSwitch devices with no PAM tooling, generate unique passwords using 'openssl rand -base64 16' per device and document in an offline encrypted spreadsheet (KeePass) until a secrets manager is available. After rotation, verify no pre-shared keys or default credentials remain via 'show full-configuration | grep password' on each managed device.

Evidence: Capture before initiating upgrade: (1) Full FortiGate configuration backup ('execute backup config ftp ') to preserve pre-patch state as forensic baseline; (2) Running process list ('diag sys process list') and loaded kernel modules ('diag sys mpstat') to document the pre-patch CAPWAP daemon binary hash and memory state; (3) List of all managed device credentials currently in use ('show wireless-controller wtp' and 'show switch-controller

managed-switch' including pre-shared-key fields) to establish rotation audit trail; (4) Timestamp and hash of the FortiOS firmware file being applied, retained as chain-of-custody evidence that a validated Fortinet-issued patch was installed and not a tampered image.

Step 4: Recovery — After patching, confirm the CAPWAP daemon is running the updated binary. Validate managed device re-authentication and normal CAPWAP handshake behavior in FortiGate logs. Monitor for any residual anomalous activity from previously managed devices for at least 72 hours post-patch. Re-baseline normal CAPWAP traffic patterns in your SIEM.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Verify the patched CAPWAP daemon binary version via 'diag sys process list | grep cw_acd' and confirm the binary timestamp matches the patch release date from FortiGuard FG-IR-26-123. Validate successful CAPWAP re-authentication for all managed FortiAP, FortiExtender, and FortiSwitch devices by checking 'show wireless-controller wtp-status' for 'Connected' state and confirming Join Response/Configuration Status sequence in event logs. For 72-hour monitoring without a SIEM, schedule a cron job or Task Scheduler entry to run 'diag debug crashlog read' every 4 hours and diff output against the post-patch baseline — any new crash entries for cw_acd during this window should trigger immediate escalation. Capture a new 30-minute CAPWAP traffic baseline PCAP on UDP 5246/5247 immediately post-patch for comparison against any future anomalies.

Evidence: Capture during and after recovery: (1) Post-patch FortiOS version confirmation output ('get system status') and CAPWAP daemon process details as signed evidence that the vulnerable cw_acd binary was replaced; (2) FortiGate wireless-controller event logs showing clean CAPWAP Discovery, Join Request, Join Response, and Configuration Status Update sequences for each previously isolated FortiAP and FortiExtender — absence of malformed element errors confirms normal handshake behavior; (3) A clean 'diag debug crashlog read' output timestamped immediately post-patch to serve as the no-crash baseline for the 72-hour monitoring window; (4) SIEM or manual log review output covering the 72-hour post-patch period showing no cw_acd crashes, no unexpected CAPWAP tunnel establishments from previously isolated devices, and no new administrative sessions on the FortiGate not attributable to authorized staff.

Step 5: Post-Incident — This vulnerability exposes a lateral movement path from managed edge devices to core firewall infrastructure. Review network segmentation between management plane traffic and production traffic. Evaluate whether managed device compromise detection (integrity monitoring, configuration drift alerts) is in place. Assess whether the principle of least privilege is enforced on FortiAP, FortiExtender, and FortiSwitch management accounts. Document findings for the next architecture review.

NIST Phase: Post Incident

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

Controls: NIST IR-8 (Incident Response Plan), NIST CA-7 (Continuous Monitoring), NIST SC-7 (Boundary Protection), NIST AC-6 (Least Privilege), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For management plane segmentation without enterprise SDN tooling: create a dedicated FortiGate VLAN for CAPWAP management traffic (FortiAP/FortiExtender/FortiSwitch to FortiGate) and enforce a firewall policy permitting only UDP 5246/5247 from the managed device subnet to the FortiGate management IP, blocking all other traffic — this prevents a compromised FortiAP from using the same network path to attack other infrastructure. For configuration drift detection without a commercial tool, use osquery with a scheduled query against FortiSwitch/FortiAP management APIs to snapshot running configs daily and diff against a known-good baseline stored offline; alert on any delta. For least privilege, audit FortiAP and FortiSwitch management accounts via 'show full-configuration | grep admin' and remove any accounts with 'prof-admin' or 'super_admin' profiles — managed edge devices require only the 'wifi' or 'restricted' management profile.

Evidence: Capture for lessons-learned documentation: (1) Network topology diagram annotated with the actual attack path — compromised managed device (FortiAP/FortiExtender/FortiSwitch) → CAPWAP control plane (UDP 5246) →

FortiGate cw_acd daemon — to concretely illustrate the lateral movement vector for architecture review; (2) Privilege audit output listing all management account profiles assigned to managed FortiAP, FortiExtender, and FortiSwitch devices, flagging any with elevated privileges beyond what CAPWAP operation requires; (3) Current firewall policy export showing whether management plane traffic (UDP 5246/5247) between managed devices and FortiGate was previously segmented or co-mingled with production traffic — this documents the segmentation gap that enabled the attack path; (4) Timeline of the incident from initial FortiGuard advisory publication through patch deployment, used to calculate mean time to remediate (MTTR) and identify process gaps for the IR plan update per NIST IR-8 (Incident Response Plan).

Detection Guidance

Focus detection on the CAPWAP control plane between FortiGate and managed devices. Query FortiOS event logs for CAPWAP daemon crashes, restarts, or error conditions; unexpected daemon restarts are a potential indicator of exploitation attempts. In your SIEM or log analysis tool, alert on abnormal message rates or malformed packet patterns from FortiAP, FortiExtender, or FortiSwitch source IPs to the FortiGate management interface. Treat as suspicious any unexpected process execution or new scheduled tasks on FortiGate that cannot be attributed to administrator activity; successful exploitation may surface as unexpected process spawning or configuration changes. Review FortiGate configuration change logs for unauthorized modifications following any anomalous CAPWAP event. No public IOCs or exploitation signatures have been reported as of this advisory; behavioral detection is the primary approach until signatures are published by Fortinet or threat intelligence providers.

Framework Mappings

MITRE-ATTACK

- **T1210** — Exploitation of Remote Services
- **T1068** — Exploitation for Privilege Escalation
- **T1059** — Command and Scripting Interpreter
- **T1021** — Remote Services
- **T1548** — Abuse Elevation Control Mechanism
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-6** — Least Privilege
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)

- **CM-6** — Configuration Settings
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-16** — Memory Protection
- **IR-5** — Incident Monitoring

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **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

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
T1210	Exploitation of Remote Services	Lateral-Movement
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1059	Command and Scripting Interpreter	Execution
T1021	Remote Services	Lateral-Movement
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
FortiGuard Labs | FortiGuard Center - IR Advisories	https://fortiguard.fortinet.com/psirt/FG-IR-26-123	T3
CVE-2025-31944 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-31944	T1
PSIRT Advisories	https://www.fortiguard.com/psirt	T3

Source	URL	Tier
Path confusion vulnerability in GUI - PSIRT | FortiGuard Labs	https://fortiguard.fortinet.com/psirt/FG-IR-25-910	T3
CVE-2025-0444 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-0444	T1
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-53844	T1

Generated 2026-05-12 14:09 UTC by TJS Security Command Center