INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-06 14:05 UTC

Ubiquiti UniFi OS Server: Chained Auth Bypass Flaws Enable Unauthenticated Root RCE

CVE VULNERABILITY | CRITICAL | CVSS 9.8

SCC Item ID	SCC-CVE-2026-0270
Type	CVE Vulnerability
CVE ID	CVE-2025-52665
Severity	CRITICAL
CVSS Base Score	9.8
EPSS Score	0.2660 (96th percentile)
Affected Products	Ubiquiti UniFi OS Server (specific versions unconfirmed from available data, patch applied per vendor advisory)
Published	6 hours ago
Discovery Source	Serper

Executive Summary

Ubiquiti has patched a chain of three critical vulnerabilities in UniFi OS Server that together allow an unauthenticated attacker to execute commands as root, the highest privilege level, on affected network devices with no credentials required. Any organization running UniFi OS devices with a management interface exposed to untrusted networks is at immediate risk of full device compromise. Bishop Fox has published detailed technical analysis of the exploit chain, lowering the barrier for exploitation significantly.

Technical Analysis

CVE-2025-52665 is part of a three-vulnerability chain affecting Ubiquiti UniFi OS Server. The chain begins with an authentication bypass (CWE-306: Missing Authentication for Critical Function; CWE-287: Improper Authentication) that allows an unauthenticated attacker to reach privileged functionality, followed by OS command injection (CWE-78) to achieve root-level remote code execution. MITRE ATT&CK techniques: T1190 (Exploit Public-Facing Application), T1068 (Exploitation for Privilege Escalation), T1059 (Command and Scripting Interpreter). CVSS base score: 9.8 (Critical). CVSS vector and vendor score pending vendor advisory confirmation; verify current CVSS details at NVD. EPSS score: 0.266 (96.4th percentile), indicating high likelihood of active exploitation relative to the broader CVE population. Specific affected version ranges are not confirmed in available source data; consult Ubiquiti's official security advisory directly for patched version

information. Bishop Fox's public blog post ('Popping Root on UniFi OS Server') details the full exploit chain and includes detection guidance. No independently verified in-the-wild exploitation at time of publication, but public exploit chain detail significantly compresses the time-to-exploitation window. NVD entry: https://nvd.nist.gov/vuln/detail/CVE-2025-52665.

Action Checklist

1. Step 1: Containment, Immediately restrict UniFi OS Server management interface access to trusted management VLANs or IP ranges only. Remove any direct internet exposure of the management interface. If isolation is not immediately possible, place an IPS/firewall rule blocking inbound access to UniFi management ports from untrusted networks. Reference: NIST AC-17 (Remote Access), restrict remote access to management interfaces per documented policy.
2. Step 2: Detection, Review UniFi OS Server logs for unauthenticated requests reaching privileged API endpoints, unexpected process spawning from web server or application processes, and any shell command execution events originating from the UniFi application layer. Check for new or modified accounts and unexpected outbound connections from UniFi OS devices. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting); CIS 8.2 (Collect Audit Logs). For exploit-chain-specific detection patterns, consult Bishop Fox's published analysis.
3. Step 3: Eradication, Obtain Ubiquiti's official security advisory (contact Ubiquiti support or visit Ubiquiti's security page for the latest advisory URL). Confirm the specific patched version for your UniFi OS device model and upgrade path. Apply the patch immediately. Do not rely on third-party version references. Reference: CIS 7.3 (Perform Automated Operating System Patch Management); CIS 7.4 (Perform Automated Application Patch Management).
4. Step 4: Recovery, After patching, verify the installed UniFi OS Server version matches the vendor-confirmed patched release. Audit all accounts on UniFi OS devices for unauthorized additions or privilege changes (Reference: CIS 5.1, Establish and Maintain an Inventory of Accounts; NIST AC-2, Account Management). Rotate credentials for any accounts on affected devices. Enable audit logging and monitor for anomalous behavior for at least 30 days post-remediation. Reference: D3-CRO (Credential Rotation); D3-LAM (Local Account Monitoring).
5. Step 5: Post-Incident, Conduct a management interface exposure audit across all network infrastructure. Document and enforce a policy requiring management interfaces to be accessible only from dedicated management networks (Reference: NIST AC-17; CIS 4.2, Establish and Maintain a Secure Configuration Process for Network Infrastructure). Assess whether MFA is enforced on UniFi management access as a secondary control (Reference: CIS 6.5, Require MFA for Administrative Access; D3-MFA, Multi-factor Authentication). Add UniFi OS Server to your vulnerability management tracking and confirm patch coverage going forward (Reference: CIS 7.1, Establish and Maintain a Vulnerability Management Process).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior IR leadership, legal, and potentially law enforcement if forensic evidence (unexpected outbound connections from UniFi OS devices, new root-level accounts, modified binaries, or shell histories showing command execution) confirms active or prior exploitation — CVSS 9.8 with a publicly detailed exploit chain (Bishop Fox analysis) and no authentication requirement means any confirmed IOC on an internet-exposed device constitutes a presumptive breach requiring regulatory notification assessment.
Recovery Notes	After patching and account remediation, verify the UniFi OS Server version via both the UI and `dpkg -l | grep unifi` against the Ubiquiti-confirmed patched release before returning the device to production traffic. Given that successful exploitation grants unauthenticated root access, any UniFi OS device that was network-exposed during the vulnerability window and shows exploitation IOCs should be treated as fully compromised — re-image from factory firmware rather than patching in place, as attacker-installed persistence (rootkits, modified binaries, backdoor accounts) may survive a package-level upgrade. Monitor UniFi OS syslog output and MongoDB admin account listings daily for a minimum of 30 days post-recovery, specifically watching for new account creation events, unexpected outbound connections to non-Ubiquiti cloud endpoints, and process execution anomalies from the unifi service user.
Forensic Artifacts	UniFi OS application logs at /var/log/unifi/server.log and /var/log/unifi/mongod.log — the exploit chain involves unauthenticated HTTP requests to privileged API endpoints, leaving HTTP access log entries with 200-series responses to auth-bypass routes from non-management source IPs with no Authorization header | Linux process execution audit trail via auditd execve records or /proc// snapshots — root RCE delivery would manifest as child shell processes (sh, bash, python) spawned under the unifi service UID or directly as UID 0, anomalous in normal UniFi OS operation | Filesystem modifications in /tmp/, /var/tmp/, /root/, and /etc/cron.d/ — unauthenticated root RCE exploits commonly write initial stage payloads, backdoor scripts, or persistence mechanisms to world-writable or root-owned directories immediately post-exploitation | MongoDB UniFi admin collection dump (mongo ace --eval 'db.admin.find().pretty()') — an attacker with root RCE would likely create a persistent UniFi admin account directly in MongoDB to maintain access across reboots, bypassing normal account creation audit trails | Network flow records or pcap captures on the management interface port (TCP 443/8443) for the exposure window — the exploit chain requires multiple sequential HTTP requests to chain the three vulnerabilities, producing a distinctive multi-stage unauthenticated HTTP session pattern to privileged API paths that is detectable in retrospective flow or full-packet capture analysis

Per-Action IR Details

Step 1: Containment — Immediately restrict UniFi OS Server management interface access to trusted management VLANs or IP ranges only. Remove any direct internet exposure of the management interface. If isolation is not immediately possible, place an IPS/firewall rule blocking inbound access to UniFi management ports from untrusted networks. Reference: NIST AC-17 (Remote Access) — restrict remote access to management interfaces per documented policy.

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 the upstream router or layer-3 switch, apply an ACL blocking inbound TCP to UniFi OS Server management ports (default: 443, 8443, 8080, 8880) from any source outside the designated management VLAN. On Linux-based gateway: `iptables -I FORWARD -d -p tcp --match multiport --dports 443,8443,8080,8880 ! -s -j DROP`. If no managed firewall exists, enable and configure UFW on the UniFi host itself: `ufw allow from to any port 443,8443 && ufw deny 443 && ufw deny 8443`. Verify with `nmap -sV -p 443,8443,8080,8880 ` from an untrusted segment to

confirm no response.

Evidence: Before restricting access, capture a full netstat/ss snapshot of active connections to UniFi management ports: `ss -tnp | grep -E '443|8443|8080|8880'` — any active sessions from non-management IPs at time of containment may represent an attacker already present. Capture UniFi OS application logs at `/var/log/unifi/` and system auth logs at `/var/log/auth.log` to preserve pre-containment activity. Export firewall state tables from the upstream device before rule insertion to preserve evidence of any attacker-controlled flows already traversing the network.

Step 2: Detection — Review UniFi OS Server logs for unauthenticated requests reaching privileged API endpoints, unexpected process spawning from web server or application processes, and any shell command execution events originating from the UniFi application layer. Cross-reference Bishop Fox's detection guidance published at https://bishopfox.com/blog/popping-root-on-unifi-os-server-unauthenticated-rce-chain-detection-analysis (T3 source — validate directly). Check for new or modified accounts and unexpected outbound connections from UniFi OS devices. Reference: 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), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: UniFi OS runs on a Debian-based Linux environment. Parse `/var/log/unifi/server.log` and `/var/log/unifi/mongod.log` for HTTP 200 responses to privileged API paths (e.g., `/api/`, `/proxy/`) originating from unauthenticated sessions — grep: `grep -E 'POST /api|GET /api' /var/log/unifi/server.log | grep -v 'Authorization'`. Check for child processes spawned by the UniFi Java process using `ps auxf` snapshots or audit `ausearch -c java --start today` if auditd is enabled. For process execution visibility without EDR, deploy auditd rules targeting execve syscalls by the unifi service user: `-a always,exit -F arch=b64 -S execve -F uid=unifi -k unifi_exec`. Review `/root/.bash_history` and `/home/*/.bash_history` for unexpected command sequences. Check `last` and `lastb` output for new SSH login events on the UniFi device.

Evidence: Capture the full `/var/log/unifi/` directory tree before any log rotation occurs — specifically `server.log`, `mongod.log`, and any `*.log.gz` archives. Extract HTTP access logs for UniFi's embedded web server, filtering for requests to authentication-bypass-relevant endpoints documented by Bishop Fox (unauthenticated requests to privileged API routes). Preserve `/proc//fd/` and `/proc//maps` if the process is still running to capture open file descriptors and memory-mapped libraries, which may reveal injected payloads. Collect `/tmp/` and `/var/tmp/` directory listings, as unauthenticated RCE exploits commonly stage initial payloads there. Export crontab entries for all users (`crontab -l -u root`, `crontab -l -u unifi`) and contents of `/etc/cron.d/` to detect persistence established after exploitation.

Step 3: Eradication — Apply Ubiquiti's patch for UniFi OS Server immediately. Consult the official Ubiquiti security advisory for the specific patched version and upgrade path — the exact version numbers are not confirmed in available source data and must be verified directly with Ubiquiti. Do not rely on third-party version references. Reference: CIS 7.3 (Perform Automated Operating System Patch Management); CIS 7.4 (Perform Automated Application Patch Management).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: 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), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Before patching, take a full filesystem snapshot or backup of the UniFi OS device if the hardware supports it (UDM/UDM-Pro support config backup via UI or `ubnt-tools backup`). Apply the vendor patch via the UniFi OS update mechanism: navigate to UniFi OS Settings > Updates, or for headless devices use `apt-get update &&

apt-get install --only-upgrade unifi` on the underlying Debian system after confirming the Ubiquiti apt repository is current. After patching, run `dpkg -l | grep unifi` to confirm the installed package version matches the Ubiquiti-published patched release. If any evidence of prior compromise was found in Step 2 (shells, backdoors, new accounts), do NOT patch in place — re-image the device from factory firmware, restore a pre-compromise configuration backup, and then patch to the fixed version.

Evidence: Before applying the patch, preserve the current UniFi OS package manifest (`dpkg -l > /tmp/pkg_manifest_preupgrade.txt`) and a hash of the core application JAR files (`find /usr/lib/unifi -name '*.jar' -exec sha256sum {} \; > /tmp/jar_hashes_preupgrade.txt`) to establish a pre-patch baseline for later comparison. If the system shows signs of prior exploitation (unexpected binaries, modified files), run `find / -newer /var/lib/dpkg/info/unifi.list -type f 2>/dev/null` to identify files modified after the last UniFi package update, which may indicate attacker-installed persistence. Capture `/etc/passwd`, `/etc/shadow`, and `/etc/sudoers.d/` before eradication to document any accounts or privilege grants created by an attacker leveraging the root RCE chain.

Step 4: Recovery — After patching, verify the installed UniFi OS Server version matches the vendor-confirmed patched release. Audit all accounts on UniFi OS devices for unauthorized additions or privilege changes (Reference: CIS 5.1 — Establish and Maintain an Inventory of Accounts; NIST AC-2 — Account Management). Rotate credentials for any accounts on affected devices. Enable audit logging and monitor for anomalous behavior for at least 30 days post-remediation. Reference: D3-CRO (Credential Rotation); D3-LAM (Local Account Monitoring).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Enumerate all local OS-level accounts on the UniFi device: `cat /etc/passwd | awk -F: '$3 >= 1000 || $3 == 0'` and compare against a known-good baseline. For UniFi application-layer accounts, use the UniFi OS admin UI to review all admin accounts under Settings > Admins, or query the MongoDB instance directly: `mongo --quiet ace --eval 'db.admin.find({},{name:1,role:1,_id:0}).pretty()'`. Force password rotation for all admin accounts via the UI. Enable syslog forwarding from the UniFi device to a dedicated log collector (even a simple rsyslog server on a spare Linux host): configure in UniFi OS Settings > System > Remote Syslog. Deploy a daily cron job to diff `/etc/passwd` against baseline: `diff /etc/passwd /root/baseline_passwd.txt` and alert on any delta.

Evidence: Post-patch, run integrity verification on critical UniFi application binaries by comparing SHA-256 hashes of JARs and configuration files against the freshly patched package manifest generated in Step 3. Capture the current account state from both the OS layer (`/etc/passwd`, `/etc/sudoers`) and the UniFi MongoDB admin collection as a recovery baseline document. Preserve all logs collected during the incident window — `/var/log/unifi/`, `/var/log/auth.log`, `/var/log/syslog` — to offline storage with hash verification (`sha256sum /var/log/unifi/*.log > /evidence/unifi_log_hashes.txt`) before the 30-day monitoring period begins, ensuring evidence is not overwritten by log rotation.

Step 5: Post-Incident — Conduct a management interface exposure audit across all network infrastructure. Document and enforce a policy requiring management interfaces to be accessible only from dedicated management networks (Reference: NIST AC-17; CIS 4.2 — Establish and Maintain a Secure Configuration Process for Network Infrastructure). Assess whether MFA is enforced on UniFi management access (Reference: CIS 6.5 — Require MFA for Administrative Access; D3-MFA — Multi-factor Authentication). Add UniFi OS Server to your vulnerability management tracking and confirm patch coverage going forward (Reference: 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-17 (Remote Access), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure), CIS 6.5 (Require MFA for

Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory)

Compensating: Use Shodan CLI (`shodan search 'product:UniFi'`) or a self-hosted scan via nmap (`nmap -p 443,8443,8080,8880 -sV --open`) to identify any remaining internet-exposed UniFi management interfaces across your asset inventory. For MFA enforcement, verify the UniFi OS SSO / Ubiquiti account login is protected by TOTP — this is configurable under the Ubiquiti account portal (ui.com) and enforced at the cloud SSO layer for cloud-managed deployments. For standalone/local deployments, confirm admin accounts require authentication per the patched version's access controls. Codify the management VLAN restriction as a Sigma rule or firewall policy template and store in version control (git) so it applies automatically to any future UniFi device onboarded to the environment.

Evidence: For the lessons-learned record, compile a timeline from log evidence collected across Steps 2–4: first unauthenticated request to a privileged endpoint, any successful exploit execution event, persistence artifacts found, and time-to-containment. Document the full inventory of UniFi OS devices in the environment with their firmware versions at time of discovery versus patched version — this serves as evidence for vulnerability management program review and supports regulatory documentation if breach notification thresholds were met. Archive the Bishop Fox detection guidance (validated copy) alongside internal playbook updates as supporting material for audit and future training.

Detection Guidance

Focus detection on three behavioral indicators specific to this vulnerability chain. First, unauthenticated or anomalous requests to privileged UniFi OS Server API endpoints, look for HTTP requests reaching admin-level routes without a valid session token in access logs. Second, unexpected child process creation from the UniFi application or web server process, on Linux-based UniFi OS, monitor for shell processes (sh, bash, dash) spawned by the application service user or as root without a corresponding user session. Third, post-exploitation persistence indicators: new local accounts, modifications to /etc/passwd or /etc/shadow, new cron entries, SSH authorized_keys modifications, or unexpected outbound network connections from UniFi OS devices. For exploit-chain-specific detection indicators, refer to Bishop Fox's published analysis (https://bishopfox.com/blog/popping-root-on-unifi-os-server-unauthenticated-rce-chain-detection-analysis). Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and AU-2 (Event Logging) to ensure relevant event types are captured. Reference D3-SFA (System File Analysis) for monitoring system files for tampering. No campaign-specific IOCs (malware hashes, attacker IPs, C2 domains) are available because this is a vulnerability disclosure, not an active threat campaign analysis. Indicators of compromise, in this context, refer to exploitation artifacts on affected systems (new accounts, shell processes, modified files), which are detailed above.

Framework Mappings

MITRE-ATTACK

- **T1068** — Exploitation for Privilege Escalation
- **T1059** — Command and Scripting Interpreter
- **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
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A03:2021** — Injection

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **2.5** — Allowlist Authorized Software
- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1059	Command and Scripting Interpreter	Execution
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
	https://gbhackers.com/critical-unifi-os-auth-bypass-flaws/	T3
Popping Root on UniFi OS Server: Unauthenticated RCE…	https://bishopfox.com/blog/popping-root-on-unifi-os-server-unauthen...	T3
CVE-2025-52665 - RCE in Unifi Access : r/cybersecurity - Reddit	https://www.reddit.com/r/cybersecurity/comments/1omwcr3/cve20255266...	T3
Ubiquiti patches critical UniFi CVEs, requires management interface ...	https://www.linkedin.com/posts/lawrencesystems_ubiquiti-just-patche...	T3
Ubiquiti Patches Critical UniFi OS Vulnerabilities - LinkedIn	https://www.linkedin.com/posts/phil-weaver_ubiquiti-patches-three-m...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-52665	T1

Generated 2026-06-06 14:05 UTC by TJS Security Command Center