INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-22 13:51 UTC

# Ubiquiti Patches Three Maximum Severity Vulnerabilities in UniFi OS

SECURITY ANALYSIS | CRITICAL | CVSS 10.0

| | |
|---|---|
| SCC Item ID | SCC-STY-2026-0151 |
| Type | Security Analysis |
| Severity | CRITICAL |
| CVSS Base Score | 10.0 |
| Affected Products | Ubiquiti UniFi OS (specific CVE IDs and version ranges not confirmed from available sources; refer to Ubiquiti Security Advisory Bulletin 062) |
| Published | 5 hours ago |
| Discovery Source | Serper |

## Executive Summary

Ubiquiti has patched three maximum-severity vulnerabilities in UniFi OS, at least one of which enables remote account takeover without authentication. UniFi OS powers a broad range of Ubiquiti networking hardware widely deployed in enterprise, SMB, and critical infrastructure environments, making the attack surface significant. Three simultaneous CVSS 10.0 ratings from a single vendor advisory signals a systemic authentication or access control weakness, not an isolated flaw, and should prompt immediate patch prioritization for any organization running Ubiquiti infrastructure.

## Technical Analysis

Ubiquiti's Security Advisory Bulletin 062 documents three vulnerabilities in UniFi OS rated at maximum severity. Based on reporting from BleepingComputer and community disclosure, at least one flaw enables remote account takeover, mapping directly to MITRE ATT&CK T1078 (Valid Accounts) and T1190 (Exploit Public-Facing Application). The attack chain as described requires no physical access and likely requires no prior authentication, which is consistent with a CVSS 10.0 base score. UniFi OS serves as the management layer across Ubiquiti's hardware portfolio, including network switches, access points, gateways, and cameras. Compromise of the management plane gives an attacker lateral movement potential across the entire network segment the device manages. The account takeover vector suggests either an authentication bypass, an insecure direct object reference, or a broken access control condition in the UniFi OS web interface or API. Without confirmed CVE identifiers or a published CVSS vector string, the precise vulnerability class cannot be stated with certainty; the Ubiquiti community advisory (Security Advisory Bulletin 062) remains the authoritative source. The absence of CISA KEV listing at time of publication does not indicate low risk: UniFi devices are

extensively deployed in environments that may not maintain aggressive patch cycles, and proof-of-concept development for high-profile CVSS 10.0 network management flaws typically follows within days to weeks of disclosure. Organizations should treat this disclosure as a patch-now event regardless of KEV status.

## Action Checklist

1. Step 1: Assess exposure, audit your asset inventory (CIS 1.1) to identify all Ubiquiti UniFi OS-based devices, including access points, switches, gateways, Dream Machines, and NVR/camera systems; check firmware versions against Ubiquiti Security Advisory Bulletin 062 at community.ui.com
2. Step 2: Apply patches immediately, update all affected UniFi OS devices to the versions specified in Security Advisory Bulletin 062; prioritize internet-exposed management consoles and devices accessible from untrusted network segments (CIS 7.3, CIS 7.4)
3. Step 3: Restrict management plane access, verify that UniFi Network Controller and UniFi OS management interfaces are not exposed directly to the internet; enforce firewall rules limiting access to trusted administrative subnets (NIST AC-17, CIS 4.4, CIS 4.5)
4. Step 4: Rotate credentials, rotate all UniFi OS administrative account passwords and revoke any API keys or integration tokens associated with affected devices; enforce MFA on all admin accounts (NIST AC-2, CIS 6.5, D3-CRO, D3-MFA)
5. Step 5: Hunt for compromise indicators, review UniFi OS authentication logs for anomalous login events, new account creation, configuration changes, or unexpected admin sessions prior to patch deployment; correlate with perimeter logs for inbound management-plane traffic (NIST AU-6, NIST SI-4, CIS 8.2, D3-LAM)
6. Step 6: Update threat model, register T1078 (Valid Accounts) and T1190 (Exploit Public-Facing Application) as active TTPs relevant to network management infrastructure; add Ubiquiti UniFi OS to your vulnerability tracking register with patch verification milestone
7. Step 7: Monitor for follow-up disclosures, track Ubiquiti's community advisory page and CISA Known Exploited Vulnerabilities catalog for CVE assignments, exploit publication, and any active exploitation reports

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate to full IR engagement if Step 5 log analysis reveals any of the following: admin accounts created outside change management windows, successful authentication events from non-authorized source IPs to the UniFi management plane, configuration changes (firewall rules, VLAN assignments, VPN credentials) with no corresponding change record, or evidence of lateral movement from the UniFi controller host into adjacent network segments — any of these conditions indicates the unauthenticated account takeover was exploited pre-patch and the environment should be treated as compromised; additionally, if UniFi OS devices are in scope for PCI-DSS, HIPAA, or state breach notification law and compromise cannot be ruled out, legal counsel and compliance teams must be notified. |

| | |
|---|---|
| **Recovery Notes** | After patching and credential rotation, re-baseline all UniFi OS device configurations by exporting and comparing current configs against the last known-good backup predating the vulnerability disclosure window — pay particular attention to firewall rule additions, new admin accounts, VPN peer configurations, and VLAN changes that could represent attacker-established persistence. Monitor UniFi OS authentication logs daily for a minimum of 30 days post-patch for re-appearance of any anomalous source IPs identified during threat hunting, as threat actors who achieved account takeover may attempt re-entry using credentials harvested before rotation. Verify patch integrity by confirming firmware SHA-256 checksums against Ubiquiti's published values for the remediated versions listed in Bulletin 062. |
| **Forensic Artifacts** | UniFi OS system log at /var/log/messages on each device: contains authentication events, account creation/modification records, API key usage, and configuration change entries — primary artifact for detecting unauthenticated account takeover exploitation; export via SSH before any firmware upgrade as log rotation or upgrade process may overwrite entries \| UniFi Network Controller MongoDB database (self-hosted: mongodump from /usr/lib/unifi/data/db; UniFi OS native: Settings > Backup): contains historical admin session records, device adoption events, configuration change history with timestamps — allows reconstruction of the full administrative action timeline to identify attacker-introduced changes \| Perimeter firewall and/or router connection logs for inbound TCP 8443, 8080, and 443 to the UniFi controller IP: the unauthenticated account takeover attack would appear as a successful HTTP/HTTPS session to the management interface from a non-administrative source IP with no preceding failed authentication attempts — absence of auth failures before a successful session is the key anomaly signature for this vulnerability class \| UniFi OS admin account export (Settings > Admins & Users) with account creation timestamps and last-login timestamps: any account with a creation timestamp during the exploitation window (between vulnerability introduction and patch deployment) and no corresponding provisioning record is direct forensic evidence of persistence established via the account takeover vulnerability \| UniFi OS API key list and associated access logs (Settings > System > API Keys): attacker-created API keys would persist through password rotations and provide durable access even after admin password changes — keys with creation timestamps in the exploitation window or with no documented provisioning owner are high-confidence persistence indicators specific to this authentication bypass vulnerability class |

## Per-Action IR Details

**Step 1: Assess exposure — audit your asset inventory (CIS 1.1) to identify all Ubiquiti UniFi OS-based devices, including access points, switches, gateways, dream machines, and NVR/camera systems; check firmware versions against Ubiquiti Security Advisory Bulletin 062 at community.ui.com**

**NIST Phase:** Preparation

**Reference:** NIST 800-61r3 §2 — Preparation: Establishing IR capability requires knowing what assets are at risk before an incident occurs

**Controls:** NIST RA-2 (Security Categorization), NIST CM-8 (System Component Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported)

**Compensating:** Run a network sweep using `nmap -sV --script banner -p 80,443,8080,8443 ` to fingerprint UniFi management interfaces; supplement with `ubnt-discover` (Ubiquiti Discovery Tool, free) to enumerate all UniFi devices on Layer 2 segments. Cross-reference discovered hostnames and MACs against your DHCP lease log at `/var/lib/dhcp/dhcpd.leases` or equivalent. Document firmware version reported in UniFi OS dashboard under Settings > System > Updates for each device.

**Evidence:** Before any patching action, snapshot the current firmware version string from each device via the UniFi OS dashboard or SSH (`cat /etc/version` or `ubnt-tools info`); preserve this as your pre-patch baseline to confirm scope

and to establish a before/after forensic record if compromise is later suspected on a specific device.

**Step 2: Apply patches immediately — update all affected UniFi OS devices to the versions specified in Security Advisory Bulletin 062; prioritize internet-exposed management consoles and devices accessible from untrusted network segments (CIS 7.3, CIS 7.4)**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 — Containment Strategy: Patching removes the vulnerable attack surface for unauthenticated remote account takeover; internet-exposed consoles represent the highest-priority containment action

**Controls:** NIST SI-2 (Flaw Remediation), NIST CM-3 (Configuration Change Control), 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)

**Compensating:** If automated patching is unavailable, use the UniFi OS web UI (Settings > System > Updates) or SSH to manually trigger firmware upgrades sequentially, starting with any Dream Machine Pro, Dream Router, or UniFi OS Console devices that host the management plane. For devices without direct internet access, download the firmware `.bin` file from Ubiquiti's firmware download portal and use the manual upgrade path in the UI. Log each device's pre- and post-patch firmware version in a change record (even a dated spreadsheet) to satisfy NIST CM-3 documentation requirements.

**Evidence:** Before patching each device, export the current UniFi OS system log via SSH (`grep -i 'auth\|login\|admin\|account\|api' /var/log/messages`) and preserve a full config backup (Settings > System > Backup in UniFi OS) as forensic baseline. These logs will be overwritten or rotated post-upgrade and are critical for retrospective compromise analysis if an account takeover is later discovered.

**Step 3: Restrict management plane access — verify that UniFi Network Controller and UniFi OS management interfaces are not exposed directly to the internet; enforce firewall rules limiting access to trusted administrative subnets (NIST AC-17, CIS 4.4, CIS 4.5)**

**NIST Phase:** Containment

**Reference:** NIST 800-61r3 §3.3 — Containment Strategy: Network-level isolation of the UniFi management plane limits the exploit surface for the unauthenticated account takeover vector even before patching completes

**Controls:** NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

**Compensating:** Query Shodan (free account) for your public IP ranges filtered on UniFi management ports (TCP 8443, 8080, 443) to confirm external exposure before and after firewall changes. On the UniFi gateway itself, apply a `firewall modify` rule (EdgeOS) or a traffic rule in UniFi Network to block inbound TCP 8443/8080 from WAN to the controller host. Verify the block with `nmap -p 8443,8080 ` from an external host. If UniFi OS Remote Access (ui.com cloud relay) is enabled, assess whether disabling it is operationally feasible during the patch window — this eliminates the cloud-proxied attack surface entirely.

**Evidence:** Pull firewall connection tracking logs or perimeter router NetFlow/sFlow data for inbound connections to TCP 8443, 8080, and 443 targeting the UniFi controller IP in the 30 days prior to this advisory. Any source IPs establishing sessions to the management plane from non-administrative subnets — especially successful authentications — are high-priority IOCs for the unauthenticated account takeover described in Bulletin 062.

**Step 4: Rotate credentials — rotate all UniFi OS administrative account passwords and revoke any API keys or integration tokens associated with affected devices; enforce MFA on all admin accounts (NIST AC-2, CIS 6.5, D3-CRO, D3-MFA)**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication: Because at least one vulnerability enables unauthenticated remote account takeover, all existing credentials must be treated as potentially compromised and rotated as part of threat removal

**Controls:** NIST AC-2 (Account Management), NIST AC-3 (Access Enforcement), NIST IA-5 (Authenticator Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process), CIS 6.5 (Require MFA for Administrative Access)

**Compensating:** Export the current admin account list from UniFi OS (Settings > Admins & Users) before rotation and compare it against your authorized admin roster — any account not on the roster is a potential persistence artifact from the account takeover vulnerability. Revoke all API keys under Settings > System > API Keys. For MFA, UniFi OS supports TOTP natively; enable it for all local admin accounts via Settings > Admins > [user] > Two-Factor Authentication. If using Ubiquiti SSO (ui.com accounts), enforce MFA at the ui.com account level as well, since cloud-linked credentials would also be exposed.

**Evidence:** Before rotating credentials, export the full admin account list including creation timestamps and last-login timestamps from UniFi OS. Any admin account created after the advisory disclosure date (or within the exploitation window identified in log analysis) with no corresponding change management record is forensic evidence of account persistence established via the unauthenticated takeover vector. Preserve this export as a signed artifact with a hash before making changes.

**Step 5: Hunt for compromise indicators — review UniFi OS authentication logs for anomalous login events, new account creation, configuration changes, or unexpected admin sessions prior to patch deployment; correlate with perimeter logs for inbound management-plane traffic (NIST AU-6, NIST SI-4, CIS 8.2, D3-LAM)**

**NIST Phase:** Detection Analysis

**Reference:** NIST 800-61r3 §3.2 — Detection and Analysis: Active threat hunting against UniFi OS authentication and configuration logs is required to determine whether the unauthenticated account takeover was exploited before patch deployment

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

**Compensating:** SSH into each UniFi OS device and run: `grep -iE '(login|auth|admin|account|create|modify|password|api_key)' /var/log/messages | grep -v 'INFO' > /tmp/unifi_auth_hunt.txt`. Look specifically for login events from non-administrative source IPs, account creation events with no corresponding change ticket, and configuration modification events outside business hours. Correlate source IPs from these logs against your firewall's inbound connection log for TCP 8443/8080 using: `grep '' /var/log/firewall.log | awk '{print $NF}' | sort | uniq -c | sort -rn`. Flag any source IP that established a management session and is not in your authorized admin IP list — these are your highest-priority IOCs for the unauthenticated takeover.

**Evidence:** Collect and preserve the following before any log rotation occurs: (1) `/var/log/messages` from all UniFi OS devices for the 90 days preceding the patch — this contains authentication events, account changes, and configuration modifications; (2) UniFi Network Controller database backup (`mongodump` if self-hosted, or Settings > Backup for UniFi OS native controller) which contains historical device association, admin session, and config change records; (3) perimeter firewall logs for inbound TCP 8443, 8080, and 443 to the controller IP covering the same window.

**Step 6: Update threat model — register T1078 (Valid Accounts) and T1190 (Exploit Public-Facing Application) as active TTPs relevant to network management infrastructure; add Ubiquiti UniFi OS to your vulnerability tracking register with patch verification milestone**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity: Lessons-learned and threat model updates ensure that the systemic authentication weakness pattern in UniFi OS informs detection engineering and future risk assessments for network management infrastructure

**Controls:** NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST PM-16 (Threat Awareness Program), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

**Compensating:** Add a Sigma detection rule targeting UniFi management plane authentication failures and new account creation events to your log analysis pipeline (Sigma rule category: network_management, product: ubiquiti). Register MITRE ATT&CK T1078.001 (Valid Accounts: Default Accounts) and T1190 (Exploit Public-Facing Application) in your risk register with UniFi OS as the affected asset class. If you use a free vulnerability tracker (even a shared

spreadsheet or a Gitea/GitHub issue), create a tracked item for Bulletin 062 with columns for: affected device, pre-patch firmware, post-patch firmware, patch date, and verifier initials. Set a 30-day re-verification milestone to confirm no devices were missed.

**Evidence:** Document the full scope of affected devices, patch status, and any anomalous findings from Step 5 log analysis as a formal incident record — even if no compromise is confirmed. Three simultaneous CVSS 10.0 findings from a single UniFi OS advisory indicates a systemic design-level access control weakness; this record supports future architectural risk decisions about UniFi OS deployment in sensitive network segments.

**Step 7: Monitor for follow-up disclosures — track Ubiquiti's community advisory page and CISA Known Exploited Vulnerabilities catalog for CVE assignments, exploit publication, and any active exploitation reports**

**NIST Phase:** Post Incident

**Reference:** NIST 800-61r3 §4 — Post-Incident Activity: Continuous monitoring for CVE assignments, public exploit code, and KEV catalog additions enables rapid re-escalation if exploitation moves from theoretical to active

**Controls:** NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-5 (Vulnerability Monitoring and Scanning), NIST AU-13 (Monitoring for Information Disclosure), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

**Compensating:** Set up a free RSS feed monitor (e.g., Feedly free tier or `rss2email`) for the Ubiquiti Community Security Advisory page (community.ui.com) and the CISA KEV catalog JSON feed at `https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json`. Write a daily cron job that fetches the KEV JSON and greps for 'ubiquiti' or 'unifi': `curl -s https://www.cisa.gov/sites/default/files/feeds/known_exploited_vulnerabilities.json | python3 -c "import sys,json; [print(v) for v in json.load(sys.stdin)['vulnerabilities'] if 'ubiquiti' in v.get('vendorProject','').lower()]"`. Subscribe to the NVD email notification service filtered on vendor 'ubiquiti' to catch CVE assignments for Bulletin 062 vulnerabilities as they are published.

**Evidence:** Maintain a dated watch log of advisory page states and KEV catalog snapshots. If CVE IDs are assigned to Bulletin 062 vulnerabilities after your patch deployment, cross-reference those CVE IDs against your patched firmware versions to confirm your remediation version is confirmed-fixed — Ubiquiti advisories sometimes lag CVE NVD enrichment, and the patched version in the bulletin may differ from what NVD records.

## Detection Guidance

Focus detection on the UniFi OS management plane. Query authentication logs for: (1) successful logins from unexpected IP addresses or geographies, especially on administrative accounts; (2) account creation or privilege escalation events not initiated through your change management process; (3) configuration changes to network devices, firewall rules, VLAN assignments, or wireless SSIDs outside approved change windows. If UniFi OS logs are forwarded to a SIEM, create alerts on any admin-plane authentication success from non-approved source IPs (NIST AU-6, AU-12). Check for unexpected outbound connections from UniFi OS hosts, which may indicate post-exploitation C2 activity. At the network perimeter, alert on inbound TCP traffic to UniFi controller ports (typically 8443, 8080, 8880, 6789) from untrusted sources. Review system initialization configuration for unauthorized changes to startup services (D3-SICA). Validate local admin account inventory against expected baseline (D3-LAM). If account takeover is suspected prior to patch application, treat any UniFi OS admin session initiated in the prior 30 days as potentially unauthorized and review session activity under NIST AU-14. Note: confirmed IOC values (hashes, C2 infrastructure) are not publicly available from the sources provided at time of writing; monitor the Ubiquiti advisory and BleepingComputer coverage for published indicators.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| URL | `Pending — refer to Ubiquiti Security Advisory Bulletin 062 (community.ui.com/releases/Security-Advisory-Bulletin-062) and BleepingComputer coverage for published indicators` | No confirmed IOC values (IP addresses, payload hashes, C2 domains) were available in the source material at time of writing; Ubiquiti's advisory and subsequent threat intelligence reporting are the authoritative sources for any published indicators | LOW |

## Framework Mappings

### MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application

### NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity

### CIS-V8

- **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
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

### SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1078 | Valid Accounts | Defense-Evasion |

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1190 | Exploit Public-Facing Application | Initial-Access |

## Sources

| Source | URL | Tier |
|---|---|---|
| | https://www.bleepingcomputer.com/news/security/ubiquiti-patches-thr... | T3 |
| **Max severity Ubiquiti UniFi flaw may allow account takeover - Reddit** | https://www.reddit.com/r/sysadmin/comments/1ry39us/patch_your_gear_... | T3 |
| **Security Advisory Bulletin 062 \| Ubiquiti Community** | https://community.ui.com/releases/Security-Advisory-Bulletin-062-06... | T3 |
| **Max severity Ubiquiti UniFi flaw may allow account takeover** | https://www.bleepingcomputer.com/news/security/ubiquiti-warns-of-un... | T3 |
| **Ubiquiti Patches UniFi Network Application Vulnerabilities - LinkedIn** | https://www.linkedin.com/posts/jnitterauer_max-severity-ubiquiti-un... | T3 |



Generated 2026-05-22 13:51 UTC by TJS Security Command Center