INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:37 UTC

Ubiquiti UniFi Network Application Critical Vulnerabilities (CVE-2026-22557, CVE-2026-22558)

CVE VULNERABILITY | **CRITICAL** | CVSS 10.0

SCC Item ID	SCC-CVE-2026-0021
Type	CVE Vulnerability
CVE ID	CVE-2026-22557, CVE-2026-22558
Severity	CRITICAL
CVSS Base Score	10.0
Affected Products	Ubiquiti UniFi Network Application (specific versions not confirmed from available raw data, refer to Ubiquiti Security Advisory Bulletin 062 for patched version details)
Published	2026-03-19

Executive Summary

Two critical vulnerabilities (CVE-2026-22557, CVSS 10.0; CVE-2026-22558) were disclosed in the Ubiquiti UniFi Network Application, with Ubiquiti issuing an emergency fix that signals high exploitability or confirmed active exploitation risk. Organizations running UniFi Network Application are exposed to unauthorized access to network infrastructure management, a compromise could give attackers control over network segmentation, traffic routing, and connected devices. Immediate patching is required; the emergency response cadence from Ubiquiti elevates this above routine vulnerability management.

Technical Analysis

CVE-2026-22557 carries a CVSS base score of 10.0 (critical), indicating network-exploitable, low-complexity, no-authentication-required access. CVE-2026-22558 was disclosed in the same advisory cycle (Ubiquiti Security Advisory Bulletin 062). Precise technical mechanism, authentication bypass, RCE, or injection class, cannot be confirmed from available data; the source fragment is partially truncated. CWE candidates are unconfirmed but plausible candidates include CWE-287 (Improper Authentication) or CWE-306 (Missing Authentication for Critical Function). MITRE ATT&CK mapping is unconfirmed; T1190 (Exploit Public-Facing Application) is plausible if network-facing exploitation is validated. Affected version ranges and exact patched versions are not confirmed from available data, verify directly against Ubiquiti Security Advisory Bulletin 062 at community.ui.com. EPSS score is not yet populated (0.0), which may reflect NVD processing lag rather than low risk. NVD entries for both CVEs should be monitored for updated scoring and technical detail. Source quality

score for this item is 0.54, treat technical specifics as preliminary until the official advisory is reviewed.

Action Checklist

1. Step 1, Patch immediately: Review Ubiquiti Security Advisory Bulletin 062 (community.ui.com/releases/Security-Advisory-Bulletin-062-062/c29719c0-405e-4d4a-8f26-e343e99f931b) to identify the patched version and update all UniFi Network Application instances without delay.
2. Step 2, Isolate internet-exposed controllers: If your UniFi Network Application is reachable from the internet or untrusted networks, restrict access via firewall rules or VPN-gating until patching is confirmed complete.
3. Step 3, Inventory all instances: Identify every UniFi Network Application deployment across your environment, including shadow IT, branch offices, and managed service clients; confirm each version against the advisory's affected range.
4. Step 4, Review access logs for unauthorized activity: Examine UniFi controller logs and network authentication logs for anomalous logins, configuration changes, or device re-associations occurring before patch application, establish a review window covering at least the past 30 days.
5. Step 5, Notify stakeholders and update controls: Inform network operations, IT leadership, and (if applicable) managed service clients of the exposure window. Document patch completion. Review whether UniFi controllers are included in your external attack surface monitoring and internet-facing asset inventory.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm or law enforcement if audit logs reveal unauthorized admin access, API calls targeting authentication services, configuration changes to network segmentation policies, or successful device provisioning outside normal maintenance windows during the 30-day review window.
Recovery Notes	After patching is confirmed complete across all instances, conduct post-incident review to validate that no configuration drift, rogue access points, or unauthorized network policies were deployed during the exposure window. Implement continuous monitoring via Ubiquiti's controller audit logging (enable in Settings > Maintenance > Logs) and integrate with SIEM if available, or parse logs manually weekly. Schedule quarterly inventory audits of UniFi deployments and enforce change control requiring firewall rules blocking internet-direct access to all controllers.
Forensic Artifacts	/usr/lib/unifi/logs/system.log (UniFi authentication, admin API calls, device events) | /usr/lib/unifi/logs/mongod.log (MongoDB transaction log, database modifications) | UniFi controller backup export (Settings > Backup) — contains historical configuration and version metadata | Network DHCP server logs (/var/lib/dhcp/dhcpd.leases or Windows Event Viewer DHCP) — detects unauthorized device provisioning | Switch/wireless AP syslog entries and authentication logs — identifies unauthorized network device logins and configuration changes

Per-Action IR Details

Step 1 — Patch immediately: Review Ubiquiti Security Advisory Bulletin 062 (community.ui.com/releases/Security-Advisory-Bulletin-062-062/c29719c0-405e-4d4a-8f26-e343e99f931b) to identify the patched version and update all UniFi Network Application instances without delay.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: tools, processes, and readiness)

Controls: NIST SI-2 (Flaw Remediation), CIS 3.12 (Address Unauthorized Software)

Compensating: If Ubiquiti advisory is inaccessible, cross-reference CVE-2026-22557 and CVE-2026-22558 on NVD (nvd.nist.gov/vuln/detail/CVE-2026-22557); extract patched version from vendor release notes or contact Ubiquiti support directly. Document the patched version number in a change log before deployment.

Evidence: Capture current running UniFi version via SSH or CLI (`unifi-os show`), export controller configuration backup (`Settings > Backup` in UI), and photograph system information page showing installed version, build date, and last update timestamp.

Step 2 — Isolate internet-exposed controllers: If your UniFi Network Application is reachable from the internet or untrusted networks, restrict access via firewall rules or VPN-gating until patching is confirmed complete.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.2 (Containment: limit scope and impact)

Controls: NIST AC-3 (Access Enforcement), NIST SC-7 (Boundary Protection), CIS 1.2 (Remove Unnecessary Ports and Services)

Compensating: Use host-based firewall (iptables on Linux, Windows Firewall) to block inbound access to UniFi ports (default 8443 HTTPS, 8080 HTTP, 27117 MongoDB) except from authorized admin IPs; document allowed IPs in a static file. Alternatively, require SSH tunneling or bastion host access: `ssh -L 8443:localhost:8443 admin@unifi-controller` from approved networks only.

Evidence: Before isolating, export netstat/ss output showing listening ports and active connections (`netstat -tlnp | grep java`), capture firewall rule baseline with current inbound/outbound policies, and record DNS resolution history for UniFi controller FQDN to identify external resolution patterns (check UniFi logs and DNS server logs for the past 30 days).

Step 3 — Inventory all instances: Identify every UniFi Network Application deployment across your environment, including shadow IT, branch offices, and managed service clients; confirm each version against the advisory's affected range.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Detection and Analysis: determine scope)

Controls: NIST CM-8 (Information System Component Inventory), CIS 2.1 (Enable CMOD for All Assets)

Compensating: Without asset management tools, manually audit network subnets using nmap to discover UniFi controllers: `nmap -p 8443 --script ssl-cert 10.0.0.0/8 | grep -i unifi`. Cross-reference results with network diagrams, firewall rules, and contact branch office/client IT leads. Create a spreadsheet with hostname, IP, version, and deployment date for tracking.

Evidence: Capture output of controller discovery scan (nmap, ping sweep results), extract SSL certificates from each UniFi instance to verify hostname and issue date, retrieve version strings from HTTP headers (`curl -I https://:8443`), and document admin account creation/modification timestamps from UniFi controller logs (`/usr/lib/unifi/logs/mongod.log` or via UI).

Step 4 — Review access logs for unauthorized activity: Examine UniFi controller logs and network authentication logs for anomalous logins, configuration changes, or device re-associations occurring before patch application — establish a review window covering at least the past 30 days.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Detection and Analysis: investigation and data collection)

Controls: NIST AU-2 (Audit Events), NIST AU-6 (Audit Review, Analysis, and Reporting), CIS 8.2 (Collect Detailed Audit Logs)

Compensating: Export UniFi controller logs: `unifi-os ssh systemctl logs unifi | tail -10000 > unifi_logs.txt` (or access `/usr/lib/unifi/logs/system.log` directly). Parse for login failures, admin account creation, and network device changes using grep: `grep -i 'login\|unauthorized\|admin\|device' unifi_logs.txt`. Cross-reference with network device MAC address changes and DHCP lease logs to detect mass re-associations.

Evidence: Capture full 30-day UniFi controller audit logs including authentication events, admin API calls, and device provisioning records. Export network DHCP server logs (ISC DHCP: `/var/lib/dhcp/dhcpd.leases`; Windows DHCP: Event Viewer > System > DHCP). Collect switch/AP syslog entries for login attempts and configuration changes. Extract browser cookies and session tokens from any admin access points to identify session hijacking. Preserve MongoDB transaction logs if available (`/usr/lib/unifi/logs/mongod.log`) to detect unauthorized database writes.

Step 5 — Notify stakeholders and update controls: Inform network operations, IT leadership, and (if applicable) managed service clients of the exposure window. Document patch completion. Review whether UniFi controllers are included in your external attack surface monitoring and internet-facing asset inventory.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.2.5 (Post-Incident Activities: lessons learned, communication)

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST CA-7 (Continuous Monitoring), CIS 6.3 (Address Unauthorized Software)

Compensating: Create incident log entry documenting: discovery date, affected versions, CVE identifiers, patching timeline, and confirmation that no exploitation was detected. Send email notification template to stakeholders with patch version, deployment deadline, and verification steps. Use free OSINT tools (Shodan, Censys, Zoomeye) to verify UniFi controller FQDN is not publicly indexed; if found, document removal request with search engine.

Evidence: Document patch deployment log (start time, systems patched, completion timestamp, verification results). Preserve pre- and post-patch version inventory spreadsheet. Archive notification emails and stakeholder acknowledgment receipts. Capture screenshots of patched version confirmation from UI (`Settings > System > About`). Retain evidence tags and investigation notes for compliance audit trail.

Detection Guidance

Specific IOCs are not available for these CVEs from current sources. Focus detection on behavioral indicators within UniFi controller logs and adjacent network telemetry. Look for: (1) unexpected admin account creation or privilege changes in the UniFi controller audit log; (2) configuration changes (VLAN edits, firewall rule modifications, SSID changes) with no corresponding change ticket; (3) device adoptions of unknown access points or switches not initiated by your team; (4) authentication events from unexpected source IPs, particularly against the controller management port (default TCP 8443, 8080); (5) controller process anomalies or unexpected outbound connections from the host running UniFi Network Application. If your SIEM ingests UniFi syslog output, alert on any admin-level action from IPs outside your management network. NVD entries for CVE-2026-22557 and CVE-2026-22558 should be monitored for published PoC or exploit signatures that would enable rule-based detection.

Framework Mappings

NIST-800-53R5

- **IA-2** — Identification and Authentication (Organizational Users)
- **IR-5** — Incident Monitoring

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

HIPAA-SECURITY

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

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC6.3** — Authorizes, modifies, or removes access

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

Sources

Source	URL	Tier
	https://borncity.com/win/2026/03/20/ubiquiti-unifi-network-applicat...	T3
Security Advisory Bulletin 062 | Ubiquiti Community	https://community.ui.com/releases/Security-Advisory-Bulletin-062-06...	T3
update your UniFi network applications (CVE-2026-22557, rated 10)	https://www.reddit.com/r/UNIFI/comments/1rxhb1f/psa_update_your_uni...	T3
Ubiquiti UniFi Network Application: Critical weakness allows ... - Heise	https://www.heise.de/en/news/Ubiquiti-UniFi-Network-Application-Cri...	T3
Ubiquiti rushes out emergency fix for critical bug in UniFi Network ...	https://cybernews.com/security/ubiquiti-unifi-network-application-c...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-22557, CVE-2026-22558	T1

Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-03-29 18:37 UTC by TJS Security Command Center