INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-10 08:12 UTC

Critical UniFi OS bug lets hackers gain root without authentication

SECURITY ANALYSIS | CRITICAL | CVSS 9.8

SCC Item ID	SCC-STY-2026-0187
Type	Security Analysis
Severity	CRITICAL
CVSS Base Score	9.8
Affected Products	Ubiquiti UniFi OS Server (specific versions not confirmed from available source data)
Published	6 hours ago
Discovery Source	Serper

Executive Summary

Researchers at Bishop Fox have disclosed a chained exploit against Ubiquiti UniFi OS Server that allows an unauthenticated attacker to gain root-level control of affected devices with no credentials required. The attack combines three vulnerabilities: missing authentication (CWE-306), code injection (CWE-94), and command injection (CWE-78), into a single exploit chain. Affected version ranges have not been confirmed from available source data; consult Ubiquiti's official security advisory to determine which versions in your environment are at risk. Any organization running unpatched UniFi OS Server hardware exposed to untrusted networks faces a complete device compromise risk, including network infrastructure takeover.

Technical Analysis

Bishop Fox researchers disclosed an unauthenticated remote code execution chain targeting Ubiquiti UniFi OS Server. The chain exploits three weaknesses in sequence: CWE-306 (missing authentication for a critical function), CWE-94 (code injection), and CWE-78 (OS command injection), mapped to MITRE ATT&CK T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), and T1068 (Exploitation for Privilege Escalation). The end result is unauthenticated root-level RCE on the device. A CVSS base score of 9.8 (Critical) reflects the no-authentication, network-accessible attack vector; this score is derived from attack vector analysis and is not yet formally scored by NVD. Specific CVE IDs and affected version ranges have not been confirmed in available source data and must be verified against NVD and Ubiquiti's official security advisory before patching. Ubiquiti has reportedly released fixes; unpatched deployments remain fully exposed. Primary technical reference: Bishop Fox blog post 'Popping Root on UniFi OS Server: Unauthenticated RCE Chain

Detection Analysis' (bishopfox.com/blog/popping-root-on-unifi-os-server-unauthenticated-rce-chain-detection-analysis). CVE ID(s) have not been assigned or confirmed as of publication date.

Action Checklist

1. Step 1: Containment. Immediately identify all UniFi OS Server instances in your environment (CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory). Restrict management interface access to trusted internal networks or a dedicated management VLAN. Block external access to UniFi OS management ports at the perimeter firewall until patching is confirmed complete (NIST AC-4: Information Flow Enforcement).
2. Step 2: Detection. Query firewall and network logs for unexpected inbound connections to UniFi OS management interfaces from untrusted source IPs. Review UniFi OS system logs for anomalous process spawning, unexpected root-level shell activity, or unfamiliar cron/init entries. Apply D3-SFA (System File Analysis), check system executables, init configuration, and auth logs for signs of tampering. Apply D3-SICA (System Init Config Analysis) for persistence indicators in startup configuration. Specific IOC patterns and log signatures have not been confirmed from available source data; reference the Bishop Fox detection analysis for behavioral anomalies to monitor.
3. Step 3: Eradication. Consult Ubiquiti's official security advisory at ui.com/security to identify confirmed patched versions for your deployment. Apply all patches specified in the advisory for UniFi OS Server immediately. Do not assume all updates address this vulnerability chain, verify version numbers against the advisory before deploying. Disable any unused or unnecessary services on the UniFi OS management interface (NIST AC-6: Least Privilege).
4. Step 4: Recovery. After patching, verify the installed UniFi OS version matches the vendor-confirmed patched release specified in Ubiquiti's advisory. Rotate all administrative credentials for UniFi OS and any downstream network devices managed through the platform (D3-CRO: Credential Rotation). Re-audit management interface access controls and confirm firewall rules restrict access to authorized management hosts only (NIST AC-17: Remote Access; CIS 4.4: Implement and Manage a Firewall on Servers). Monitor for post-compromise persistence indicators for at least 30 days.
5. Step 5: Post-Incident. Review network segmentation controls to ensure management interfaces are isolated from production and internet-facing segments (NIST AC-4: Information Flow Enforcement; CIS 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure). Evaluate whether management authentication enforcement (NIST AC-3: Access Enforcement; D3-MFA: Multi-factor Authentication) is applied consistently across all network infrastructure. Document this event in your vulnerability management process (CIS 7.1: Establish and Maintain a Vulnerability Management Process) and schedule recurring review of Ubiquiti security advisories.

Detection Guidance

The following detection guidance is based on the attack chain description. Specific IOC hashes, log event IDs, and network signatures have not been confirmed from available source data; monitor for behavioral anomalies matching the attack chain rather than relying on confirmed signatures. Query firewall and network flow logs for inbound connections to UniFi OS management ports (default TCP 443, 8443, 8080; verify against your deployment) from untrusted or external source addresses. On the UniFi OS device, review /var/log/auth.log and

system logs for unexpected root-level process execution or shell spawning not initiated by a known admin session. Apply D3-SFA (System File Analysis): compare system executables and configuration files against known-good baselines for modification or tampering. Apply D3-SICA (System Init Config Analysis): inspect startup and cron configurations for unauthorized persistence entries. Apply D3-LAM (Local Account Monitoring): look for new or modified local accounts with elevated privileges. Reference the Bishop Fox blog post (bishopfox.com/blog/popping-root-on-unifi-os-server-unauthenticated-rce-chain-detection-analysis) for detailed detection analysis and technical indicators.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://bishopfox.com/blog/popping-root-on-unifi-os-server-unauthenticated-rce-chain-detection-analysis`	Primary technical research source — Bishop Fox exploit chain and detection analysis	HIGH

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter
- **T1068** — Exploitation for Privilege Escalation

NIST-800-53R5

- **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
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (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

- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **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

MITRE ATT&CK Mapping

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

Sources

Source	URL	Tier
	https://www.bleepingcomputer.com/news/security/critical-unifi-os-bu...	T3
Critical UniFi OS bug lets hackers gain root without authentication	https://www.reddit.com/r/SecOpsDaily/comments/1u0cbmt/critical_unif...	T3
Popping Root on UniFi OS Server: Unauthenticated RCE…	https://bishopfox.com/blog/popping-root-on-unifi-os-server-unauthen...	T3
5 Critical UniFi CVEs and How to Avoid the Risk - YouTube	https://www.youtube.com/watch?v=6DAhg6-9wvg	T3
Critical UniFi OS Vulnerabilities Allow ... - Instagram	https://www.instagram.com/p/DZQQhuskQlV/	T3

Generated 2026-06-10 08:12 UTC by TJS Security Command Center