INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-24 19:00 UTC

CISA Flags Active Exploitation of Max-Severity Flaws in Ubiquiti UniFi OS and Lantronix Serial-to-Ethernet Devices

CVE VULNERABILITY | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CVE-2026-0345
Type	CVE Vulnerability
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Ubiquiti UniFi OS (network infrastructure platforms); Lantronix serial-to-Ethernet servers (serial device servers)
Published	2026-06-24T10:35:15
Discovery Source	Rss

Executive Summary

CISA has issued an active exploitation warning for critical vulnerabilities in Ubiquiti UniFi OS network infrastructure and Lantronix serial-to-Ethernet devices, with CVSS scores reaching 9.5. Attackers can gain unauthenticated remote code execution and root-level access to affected network equipment without valid credentials. Organizations running these platforms, particularly those in operational technology and healthcare environments, face immediate risk of network compromise, persistent backdoor access, and potential disruption to legacy systems bridged through Lantronix converters.

Technical Analysis

CISA has flagged active in-the-wild exploitation of multiple critical vulnerability classes affecting two device families. Affected platforms: Ubiquiti UniFi OS Server (network infrastructure management platform) and Lantronix serial-to-Ethernet device servers (serial-to-IP converters used in OT and healthcare).

Weakness classes confirmed across both platforms:

- CWE-306: Missing Authentication for Critical Functions, allows unauthenticated access to privileged operations

- CWE-78: OS Command Injection, enables injection of arbitrary OS commands through unsanitized input

- CWE-120: Classic Buffer Overflow, memory corruption enabling arbitrary code execution

- CWE-287: Improper Authentication, authentication bypass permitting unauthorized access

CVSS base score: 9.5 (Critical). CVSS vector string is pending NVD publication. EPSS data not yet available in source material.

CVE-2026-47368 has been referenced in third-party sources (CyCognito) as an information disclosure via path traversal affecting UniFi OS. Bishop Fox has publicly documented an unauthenticated RCE chain against UniFi OS Server achieving root privilege escalation.

MITRE ATT&CK techniques mapped: T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), T1068 (Exploitation for Privilege Escalation), T1133 (External Remote Services), T1078 (Valid Accounts), T1016 (System Network Configuration Discovery), T1565.002 (Transmitted Data Manipulation).

Lantronix serial-to-IP converters present elevated OT and healthcare risk because they bridge legacy serial equipment to IP networks; compromise enables access to downstream legacy systems with no independent authentication layer.

CISA KEV addition is signaled but not yet confirmed in source data as of the configuration date. Federal agencies subject to BOD 22-01 should prepare for a mandatory 21-day remediation deadline upon official KEV listing. Specific patch versions and vendor advisory identifiers were not available in the provided source material; operators should check Ubiquiti's security advisories and Lantronix's support portal directly.

Action Checklist

1. Step 1: Containment. Immediately identify all Ubiquiti UniFi OS Server instances and Lantronix serial-to-Ethernet devices in your environment (reference CIS 1.1, Establish and Maintain Detailed Enterprise Asset Inventory). Place internet-facing instances behind a restrictive firewall rule (CIS 4.4, Implement and Manage a Firewall on Servers) and block inbound unauthenticated access to UniFi OS management interfaces at the network perimeter. Isolate Lantronix converters from direct internet exposure; segment them onto dedicated OT/healthcare VLANs if not already done.
2. Step 2: Detection. Query firewall and network logs for unexpected inbound connections to UniFi OS management ports and Lantronix serial server ports. Review authentication logs for anonymous or unauthenticated session attempts against these devices (NIST AU-2, Event Logging; NIST AU-6, Audit Record Review, Analysis, and Reporting). Search for anomalous OS-level command execution originating from UniFi OS processes. Monitor for path traversal patterns (e.g., '../' sequences) in HTTP request logs to UniFi OS endpoints, consistent with CVE-2026-47368. Enable or verify SIEM alerting on T1190 and T1068 ATT&CK technique indicators. Apply D3-LAM (Local Account Monitoring) to detect newly created or modified local accounts on affected devices post-exploitation.
3. Step 3: Eradication. Apply the latest available firmware and software updates from Ubiquiti (https://community.ui.com/releases, validate this URL before use) and Lantronix (https://www.lantronix.com/support/, validate before use) for all affected device models. Specific patch version numbers were not available in the provided source material; consult the official vendor advisory for the authoritative remediation version. After patching, rotate all credentials on affected devices (NIST AC-2, Account Management). Disable or remove any default accounts (CIS 4.7, Manage Default Accounts on Enterprise Assets and Software).
4. Step 4: Recovery. After patching, verify device firmware versions match the vendor-recommended patched release. Re-examine authentication configurations to confirm no unauthenticated access paths

remain (NIST AC-3, Access Enforcement; NIST AC-6, Least Privilege). Review all local accounts created during the exposure window and remove unauthorized accounts. Monitor affected devices for 30 days post-patch using enhanced logging (NIST AU-6) and apply system file analysis to detect residual persistence mechanisms such as modified system init configurations. Validate that Lantronix devices resume expected serial-to-IP bridging functions without anomalous traffic.

5. Step 5: Post-Incident. Document gaps exposed: unauthenticated network device management interfaces, insufficient segmentation of OT/legacy serial infrastructure, and delayed asset visibility for network appliances. Update the enterprise asset inventory to include all network infrastructure devices and serial converters (CIS 1.1). Establish or review a vulnerability management process that covers network infrastructure firmware (CIS 7.1, Establish and Maintain a Vulnerability Management Process; CIS 7.2, Establish and Maintain a Remediation Process). Conduct a formal review of remote access controls for all network management planes (NIST AC-17, Remote Access). If KEV listing is confirmed, federal agencies must validate remediation within the BOD 22-01 deadline window.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to CISO and legal/compliance if forensic evidence shows successful unauthenticated access to any UniFi OS or Lantronix device (HTTP 200 responses to path traversal URIs, new local accounts, or outbound connections from device IPs), if any Lantronix serial server bridges to a medical device network or OT control system (triggering HIPAA breach risk assessment and potential ICS incident notification), or if the organization is a federal agency with these devices listed in asset inventory (BOD 22-01 KEV remediation deadline applies).
Recovery Notes	After applying vendor firmware patches, perform a full configuration audit of every remediated UniFi OS device to confirm management interface authentication enforcement is active — unauthenticated access paths in UniFi OS have historically survived firmware upgrades when custom configuration overrides persist in `/data/`. For Lantronix devices, verify that serial port access control lists are intact and that no attacker-added port redirect rules forward serial traffic to external IPs. Maintain enhanced logging and network flow monitoring on all affected device segments for a minimum of 30 days, as root-level RCE on embedded Linux network devices enables persistent implant installation that may not be visible until the implant beacons outbound.

Forensic Artifacts	UniFi OS web server access logs (`/var/log/unifi/` or nginx access log) — look for HTTP requests containing `../` path traversal sequences, requests to internal API endpoints (`/api/`) from external source IPs without valid session tokens, and POST requests resulting in HTTP 200 responses from unauthenticated source IPs, which indicate successful RCE trigger | UniFi OS Linux layer account and authentication files — `/etc/passwd`, `/etc/shadow`, and `/root/.ssh/authorized_keys` for attacker-added root accounts or SSH keys; compare against a known-good baseline to identify persistence artifacts left by a root-level compromise | Lantronix device running configuration export — attacker-modified serial port redirect rules routing serial traffic to attacker-controlled IP addresses are the primary OT pivot artifact; these entries will not appear in network logs but are visible only in the device configuration dump | Network flow records (NetFlow/IPFIX or firewall session logs) for connections to UniFi OS management ports (TCP 8080, 8443, 6789) and Lantronix default serial server ports (TCP 2001, 3001, 10001) — the source IP, timestamp, and session duration of connections from external or unexpected internal IPs during the exploitation window constitute the primary network-layer evidence of exploitation attempts | UniFi OS init and cron persistence paths — `find /etc/init.d/ /etc/cron.d/ /etc/cron.daily/ /var/spool/cron/ -ls` output and file content hashes; root-level RCE on embedded Linux network devices commonly results in cron-based or init.d-based backdoor installation that survives service restarts and is the most common post-exploitation persistence mechanism on this device class

Per-Action IR Details

Step 1: Containment — Immediately identify all Ubiquiti UniFi OS Server instances and Lantronix serial-to-Ethernet devices in your environment (reference CIS 1.1 — Establish and Maintain Detailed Enterprise Asset Inventory). Place internet-facing instances behind a restrictive firewall rule (CIS 4.4 — Implement and Manage a Firewall on Servers) and block inbound unauthenticated access to UniFi OS management interfaces at the network perimeter. Isolate Lantronix converters from direct internet exposure; segment them onto dedicated OT/healthcare VLANs if not already done.

NIST Phase: Containment

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), NIST AC-4 (Information Flow Enforcement)

Compensating: Run `nmap -p 8080,8443,443,22,6789 ` to enumerate exposed UniFi OS management ports and `nmap -p 2001,3001,10001,30718 ` for Lantronix default serial-server ports. Use pfSense or iptables rules to immediately block inbound traffic to those ports from non-management source IPs. On Linux-based UniFi OS hosts, confirm internet exposure with `ss -tlnp | grep -E '8080|8443|6789'` and apply a host firewall rule via `ufw deny from any to any port 8080` as an interim measure until perimeter rules propagate.

Evidence: Before isolating or applying firewall rules, capture: (1) active TCP connection state from the UniFi OS host via `netstat -ano` or `ss -tunp` — this records any live attacker sessions or reverse-shell connections that will vanish on isolation; (2) running process list (`ps auxf` on UniFi OS / Linux layer) to capture any injected or spawned processes resulting from unauthenticated RCE; (3) ARP table (`arp -a`) to map lateral movement pivot points; (4) full RAM image if a memory acquisition tool (LiME kernel module) is accessible on the UniFi OS Linux layer, as root-level RCE exploitation artifacts including injected payloads and in-memory backdoors will not persist to disk. Volatile network state is destroyed the moment firewall rules block active sessions.

Step 2: Detection — Query firewall and network logs for unexpected inbound connections to UniFi OS management ports and Lantronix serial server ports. Review authentication logs for anonymous or unauthenticated session attempts against these devices (NIST AU-2 — Event Logging; NIST AU-6 — Audit Record Review, Analysis, and Reporting). Search for anomalous OS-level command execution originating from UniFi OS processes. Monitor for path traversal patterns (e.g., '../' sequences) in HTTP request logs to

UniFi OS endpoints, consistent with CVE-2026-47368. Enable or verify SIEM alerting on T1190 and T1068 ATT&CK technique indicators. Apply D3-LAM (Local Account Monitoring) to detect newly created or modified local accounts on affected devices post-exploitation.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records)

Compensating: Without a SIEM, use `grep -E '\.\./|\.\./\.\./' /var/log/nginx/access.log` (or the UniFi OS equivalent web server log path, typically `/var/log/unifi/`) to surface path traversal attempts in HTTP request logs. For Lantronix devices, pull the device's internal syslog stream via `syslog-ng` or `rsyslog` forwarding to a local collector and grep for authentication failure strings. Deploy a Sigma rule converted to a grep-compatible pattern targeting unauthenticated POST requests to UniFi OS API endpoints (`/api/` paths with HTTP 200 responses and no Authorization header). Use `last` and `lastb` on the UniFi OS Linux layer to enumerate successful and failed SSH/console logins. For Lantronix, review the web management audit log via the device's HTTP admin interface under System > Logs.

Evidence: Capture before any containment action modifies live state: (1) UniFi OS web server access logs at `/var/log/unifi/` — look for HTTP GET/POST requests with `../` sequences, unusually long URI paths, or requests to internal API endpoints from external IPs without a valid session cookie; (2) UniFi OS system auth log (`/var/log/auth.log` or `/var/log/secure`) for authentication attempts with empty or null credential fields indicating unauthenticated access exploitation; (3) Lantronix device syslog output for serial port bridging anomalies — unexpected connections to serial ports from non-authorized IP addresses indicate an attacker pivoting to OT/serial-attached devices; (4) Network flow records (NetFlow/IPFIX or firewall session logs) showing the source IP, timestamp, and byte volume of connections to UniFi OS management ports 8080/8443/6789 and Lantronix ports 2001/3001 during the suspected exploitation window.

Step 3: Eradication — Apply the latest available firmware and software updates from Ubiquiti (https://community.ui.com/releases — validate this URL before use) and Lantronix (https://www.lantronix.com/support/ — validate before use) for all affected device models. Specific patch version numbers were not available in the provided source material; consult the official vendor advisory for the authoritative remediation version. After patching, rotate all credentials on affected devices (NIST AC-2 — Account Management; D3-CRO — Credential Rotation). Disable or remove any default accounts (CIS 4.7 — Manage Default Accounts on Enterprise Assets and Software).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST AC-2 (Account Management), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Before applying firmware, snapshot the current UniFi OS configuration via `ubnt-device-firmware` CLI backup or the UniFi Network Application backup export (Settings > System > Backup) to preserve a pre-patch baseline for comparison. For Lantronix devices lacking automated update mechanisms, download firmware from the validated vendor support URL to an internal staging server, verify the SHA-256 checksum against the value published in the vendor advisory, and apply via the device's web management interface under Administration > Firmware. After patching, enumerate all local accounts on UniFi OS via the UniFi Network Application (Settings > Admins) and on Lantronix via the CLI command `show localusers` or equivalent web UI path, removing any accounts not present in your pre-incident baseline.

Evidence: Because patching overwrites firmware and credential rotation invalidates active sessions, capture before executing this step: (1) full UniFi OS filesystem snapshot of `/data/` and `/etc/` directories — these contain persist configuration files, SSH authorized_keys, and any attacker-planted cron jobs or init.d scripts that survive a reboot but may be overwritten by firmware update; (2) Lantronix device running configuration export (full config dump via CLI `show config` or web UI) to capture any attacker-modified serial port redirect rules or added user accounts; (3) hash inventory of critical UniFi OS binaries (`md5sum /usr/sbin/ubnt*`) before patching to document any pre-patch trojanized

binaries; (4) list of all local accounts and their last-modified timestamps from UniFi OS (`/etc/passwd`, `/etc/shadow`) and Lantronix admin user table — newly created root-equivalent accounts are a primary persistence mechanism for RCE-level exploits on embedded Linux devices.

Step 4: Recovery — After patching, verify device firmware versions match the vendor-recommended patched release. Re-examine authentication configurations to confirm no unauthenticated access paths remain (NIST AC-3 — Access Enforcement; NIST AC-6 — Least Privilege). Review all local accounts created during the exposure window and remove unauthorized accounts. Monitor affected devices for 30 days post-patch using enhanced logging (NIST AU-6) and apply D3-SFA (System File Analysis) to detect residual persistence mechanisms such as modified system init configurations (D3-SICA — System Init Config Analysis). Validate that Lantronix devices resume expected serial-to-IP bridging functions without anomalous traffic.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention)

Compensating: Verify patched firmware version via UniFi OS CLI: `ubnt show version` or from the UniFi Network Application dashboard under Devices > [device] > Properties. For Lantronix, confirm firmware version via the web UI under Administration > Firmware or CLI `show version`. To detect residual persistence without EDR, run `find /etc/init.d/ /etc/cron* /etc/rc.local -newer /tmp/patch_timestamp -ls` on UniFi OS Linux layer to identify any init or cron files modified after the known compromise window. For Lantronix, export and diff the post-patch running configuration against the known-good baseline captured before eradication. Monitor serial port bridging traffic with Wireshark on the network segment receiving Lantronix output — unexpected destination IPs or protocols on the bridged serial stream indicate the attacker established a persistent OT relay.

Evidence: During the 30-day enhanced monitoring window, continuously capture: (1) UniFi OS syslog output for re-emergence of path traversal patterns or unauthenticated API calls — a re-exploitation attempt against a patched device indicates either patch failure or a second, unpatched instance in the environment; (2) Lantronix serial port activity logs showing connection source IPs and byte volumes — a compromised Lantronix device used as an OT pivot will show new or unusual destination IPs in the serial-to-IP stream; (3) UniFi OS `/var/log/auth.log` for any new SSH key additions to `/root/.ssh/authorized_keys` or `/home//.ssh/authorized_keys` post-patch, which would indicate an attacker re-establishing persistence via a previously planted key; (4) network flow records for outbound beaconing from UniFi OS or Lantronix device IPs to external hosts — periodic, low-volume outbound connections at regular intervals are characteristic of a C2 implant surviving the patch cycle.

Step 5: Post-Incident — Document gaps exposed: unauthenticated network device management interfaces, insufficient segmentation of OT/legacy serial infrastructure, and delayed asset visibility for network appliances. Update the enterprise asset inventory to include all network infrastructure devices and serial converters (CIS 1.1). Establish or review a vulnerability management process that covers network infrastructure firmware (CIS 7.1 — Establish and Maintain a Vulnerability Management Process; CIS 7.2 — Establish and Maintain a Remediation Process). Conduct a formal review of remote access controls for all network management planes (NIST AC-17 — Remote Access). If KEV listing is confirmed, federal agencies must validate remediation within the BOD 22-01 deadline window.

NIST Phase: Post Incident

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), NIST AC-17 (Remote Access), NIST AU-6 (Audit Record Review, Analysis, and Reporting)

Compensating: Use a free network discovery tool such as `nmap` with the `-O` flag and service version detection (`-sV`) on all internal subnets to build or validate the asset inventory specifically for UniFi OS and Lantronix device fingerprints — UniFi OS devices respond with identifiable HTTP server headers and Lantronix devices expose a characteristic Telnet/TCP banner on port 2001. Document all discovered devices in a spreadsheet baseline including

IP, MAC, firmware version, and management interface exposure status. For the vulnerability management process, subscribe to the Ubiquiti Community release RSS feed and Lantronix security advisory mailing list to ensure future firmware advisories are captured within 24 hours of publication — this directly closes the delayed-visibility gap this incident exposed.

Evidence: Preserve for the lessons-learned record and any regulatory reporting obligation: (1) the full timeline of exploitation indicators from firewall, auth, and web server logs — specifically the first observed path traversal or unauthenticated API request timestamp versus the CISA advisory publication date, to quantify the detection latency gap; (2) the pre-incident asset inventory state versus post-incident discovery output, documenting how many UniFi OS and Lantronix devices were previously untracked; (3) for healthcare environments, preserve evidence of whether any Lantronix serial-attached medical devices or OT control systems were reachable from the compromised serial server, as this may constitute a HIPAA Security Rule incident requiring breach risk assessment under 45 CFR §164.402; (4) the patched firmware version confirmation screenshots or CLI output for each remediated device, serving as audit evidence for BOD 22-01 compliance if the vulnerabilities appear on the CISA KEV catalog.

Detection Guidance

Focus detection efforts on three surfaces: UniFi OS management interface logs, Lantronix device access logs, and downstream network telemetry.

1. Authentication anomalies: Query authentication logs on UniFi OS Server for sessions with no credential presentation or sessions where authentication steps are absent before privileged operations. Correlate with NIST AU-2 event types for logon failures and privilege use.

2. Path traversal indicators: Search HTTP access logs on UniFi OS for request URIs containing '../' or URL-encoded equivalents ('%2e%2e%2f', '%2e%2e/') consistent with CVE-2026-47368 path traversal behavior.

3. Command injection patterns: In OS-level process audit logs (where available), look for unexpected child process spawning from UniFi OS service processes, particularly shell interpreters (sh, bash) launched as child processes of web service or API service processes.

4. Buffer overflow and crash indicators: Review system logs for segmentation faults, process crashes, or unexpected restarts of UniFi OS or Lantronix daemon processes, which may indicate exploitation attempts even if unsuccessful.

5. Lateral movement from Lantronix devices: Monitor for unexpected IP traffic originating from Lantronix serial server IP addresses toward internal OT network segments or healthcare device subnets. Serial-to-IP converters should have narrowly defined traffic profiles; deviation is a strong indicator.

6. New account creation: Apply local account monitoring to look for new local accounts or SSH authorized_keys modifications on UniFi OS devices post-exposure.

7. Network-level: Correlate with T1190 (Exploit Public-Facing Application) detection rules in your SIEM. Alert on direct inbound connections from internet IP addresses to UniFi OS management ports and Lantronix serial server ports that bypass expected proxy or VPN paths.

No specific IOCs (IPs, domains, hashes) were available in the provided source material. Threat actor attribution is currently unknown.

Framework Mappings

MITRE-ATTACK

- **T1016** — System Network Configuration Discovery
- **T1133** — External Remote Services
- **T1190** — Exploit Public-Facing Application
- **T1059** — Command and Scripting Interpreter
- **T1068** — Exploitation for Privilege Escalation
- **T1565.002** — Transmitted Data Manipulation
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **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
- **AC-2** — Account Management
- **SI-16** — Memory Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **SI-10** — Information Input Validation
- **SR-2** — Supply Chain Risk Management Plan
- **IR-5** — Incident Monitoring

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
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **2.5** — Allowlist Authorized Software
- **7.3** — Perform Automated Operating System Patch Management

- **7.4** — Perform Automated Application Patch Management
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners
- **CC6.3** — Authorizes, modifies, or removes access

HIPAA-SECURITY

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

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

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1016	System Network Configuration Discovery	Discovery
T1133	External Remote Services	Persistence
T1190	Exploit Public-Facing Application	Initial-Access
T1059	Command and Scripting Interpreter	Execution
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1565.002	Transmitted Data Manipulation	Impact
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/cisa-warns-of-max-se...	T3

Source	URL	Tier
CISA warns of max severity Ubiquiti flaws exploited in attacks	https://www.linkedin.com/posts/the-cyber-security-hub_cisa-warns-of...	T3
Popping Root on UniFi OS Server: Unauthenticated RCE…	https://bishopfox.com/blog/popping-root-on-unifi-os-server-unauthen...	T3
Emerging Threat: (CVE-2026-47368) UniFi OS Information ...	https://www.cycognito.com/blog/emerging-threat-cve-2026-47368-unifi...	T3
Serial-to-IP Converter Flaws Expose OT and Healthcare Systems to ...	https://www.reddit.com/r/cybersecurity/comments/1sr4gnj/serialtoip_...	T3

Generated 2026-06-24 19:00 UTC by TJS Security Command Center