INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-30 06:31 UTC

Chained Auth Bypass Vulnerabilities in Qinglong Scheduler Actively Exploited for Cryptomining

CVE VULNERABILITY | HIGH | CVSS 7.5

SCC Item ID	SCC-CVE-2026-0097
Type	CVE Vulnerability
CVE ID	CVE-2026-3965, CVE-2026-4047
Severity	HIGH
CVSS Base Score	7.5
EPSS Score	0.0010 (28th percentile)
Affected Products	Qinglong open-source task scheduler versions 2.20.1 and older
Published	2026-04-29T16:50:35
Discovery Source	Rss

Executive Summary

Two chained authentication bypass vulnerabilities in the Qinglong open-source task scheduler are being actively exploited to install cryptomining software on affected servers. Organizations running Qinglong versions 2.20.1 or older with internet-exposed panels are at direct risk; exploitation began February 7, 2026, weeks before public disclosure. The primary business impact is server resource theft, potential lateral movement from compromised hosts, and operational disruption if affected systems run production workloads.

Technical Analysis

CVE-2026-3965 and CVE-2026-4047 (CVSS 7.5, High) affect Qinglong open-source task scheduler versions 2.20.1 and older. Both vulnerabilities stem from a mismatch between Express.js routing behavior and middleware authorization logic (CWE-288: Authentication Bypass Using an Alternate Path; CWE-863: Incorrect Authorization; CWE-94: Improper Control of Code Generation). Attackers chain the two bypasses to reach protected admin endpoints without authentication, achieving remote code execution (T1190) via shell command execution (T1059, T1059.004). Post-exploitation activity includes deploying a cryptominer disguised as a legitimate system process (T1036, T1036.005), ingress tool transfer (T1105), resource hijacking (T1496), and defense evasion by disabling security tooling (T1562, T1562.001). Exploitation predates public disclosure, suggesting prior private knowledge of the flaws. The initial maintainer patch was insufficient; the correct remediation is PR #2941. NVD records: https://nvd.nist.gov/vuln/detail/CVE-2026-3965 and

https://nvd.nist.gov/vuln/detail/CVE-2026-4047

Action Checklist

1. Step 1: Containment. Immediately restrict external access to all Qinglong panels (default port 5700) at the network perimeter. Take affected instances offline until PR #2941 is applied.
2. Step 2: Detection. Review web server and application logs for unauthenticated requests to Qinglong admin endpoints dated on or after February 7, 2026. Look for anomalous process spawning from the Qinglong service account, unexpected outbound connections, and processes masquerading as system services (T1036.005). Check CPU and resource utilization for sustained spikes consistent with cryptomining (T1496).
3. Step 3: Eradication. Apply PR #2941 to all Qinglong instances. Confirm the running version is patched beyond 2.20.1. If compromise is confirmed, treat the host as fully compromised: terminate the cryptominer process, remove dropped binaries, and audit cron jobs and scheduled tasks for persistence mechanisms.
4. Step 4: Recovery. After applying PR #2941, verify Qinglong admin endpoints reject unauthenticated requests. Monitor host resource utilization for 72 hours post-remediation to confirm cryptominer removal. Review outbound network traffic for connections to known mining pool infrastructure.
5. Step 5: Post-Incident. Assess why Qinglong panels were internet-exposed without authentication controls or network segmentation. Review the asset inventory process for open-source scheduler and admin panel exposure. Implement a policy requiring all admin panels to sit behind VPN or IP allowlisting regardless of application-layer auth.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to senior IR leadership and legal/compliance if forensic evidence confirms the cryptominer process had read access to Qinglong environment variables or scripts containing credentials, API keys, or tokens — as the auth bypass (CVE-2026-3965/CVE-2026-4047) grants full panel access, any secrets stored in Qinglong tasks must be treated as compromised, potentially triggering credential rotation obligations and, if those secrets access regulated data systems, breach notification assessment under applicable frameworks.
Recovery Notes	After applying PR #2941, confirm the patch is effective by testing that unauthenticated requests to `/api/user/profile` and `/open/auth/token` return HTTP 401/403 on every patched Qinglong instance — not just the primary host. Maintain 72-hour elevated monitoring of CPU utilization and outbound connections on port 3333/4444/5555 for all affected hosts, as cryptominer droppers frequently include a re-fetch mechanism that will reinstall the miner binary if the initial persistence (cron, systemd timer, or injected Qinglong task) was not fully eradicated. Do not return hosts to production until both the patch verification test and a clean 24-hour monitoring window have been documented.

Forensic Artifacts	Qinglong application log at `/root/ql/data/log/qinglong.log` (or `/ql/data/log/` in Docker deployments): contains HTTP request records showing unauthenticated GET/POST requests to admin API endpoints exploiting CVE-2026-3965/CVE-2026-4047 — filter for 200-series responses to `/api/user/login`, `/open/auth/token`, or `/api/scripts` without valid Authorization headers dated on or after February 7, 2026. | Crontab entries for the Qinglong service account (`/var/spool/cron/crontabs/`) and system cron directories (`/etc/cron.d/`, `/etc/cron.hourly/`): cryptominer persistence injected via the auth bypass would appear as new entries referencing base64-decoded commands, curl/wget fetches from external IPs, or execution of binaries in `/tmp` or `/dev/shm`. | Dropped cryptominer ELF binaries in world-writable directories: specifically `/tmp/`, `/dev/shm/`, `/var/tmp/`, and the Qinglong scripts directory `/root/ql/data/scripts/` — binaries will have executable permissions, no package manager provenance (`dpkg -S ` or `rpm -qf ` returns nothing), and SHA-256 hashes attributable to XMRig or similar open-source miners modified for this campaign. | Memory dump of the running miner process (captured via `gcore ` before termination): contains the embedded mining pool URL (stratum+tcp://), wallet address, and worker ID string that directly attributes the deployment to the specific threat campaign targeting Qinglong 2.20.1 and older. | Network flow or tcpdump capture showing outbound stratum protocol connections from the Qinglong host to mining pool infrastructure on TCP ports 3333, 4444, 5555, or 14444 — the stratum protocol handshake (`{"id":1,"method":"mining.subscribe"}`) is visible in plaintext in the packet payload and confirms active cryptomining rather than a dormant dropper.

Per-Action IR Details

Step 1: Containment — Immediately restrict external access to all Qinglong panels (default port 5700) at the network perimeter. If internet exposure cannot be confirmed or ruled out quickly, take affected instances offline until PR #2941 is applied. Do not rely on the initial maintainer patch.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems to prevent further exploitation while preserving evidence and maintaining availability where possible.

Controls: NIST IR-4 (Incident Handling), 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 12.1 — Ensure Network Infrastructure is Up-to-Date (network segmentation enforcement)

Compensating: On the Qinglong host, immediately apply an iptables rule to block inbound TCP/5700 from non-RFC1918 addresses: `iptables -I INPUT -p tcp --dport 5700 ! -s 10.0.0.0/8 -j DROP && iptables -I INPUT -p tcp --dport 5700 ! -s 172.16.0.0/12 -j DROP && iptables -I INPUT -p tcp --dport 5700 ! -s 192.168.0.0/16 -j DROP`. If the host is Docker-based (common Qinglong deployment), also add a UFW rule before Docker's iptables chain: `ufw insert 1 deny in on eth0 to any port 5700`. Verify with `ss -tlnp | grep 5700` and confirm no external routes resolve to the host on that port using `nmap -p 5700 ` from an external vantage point.

Evidence: BEFORE blocking port 5700, capture a full netstat/ss snapshot of active connections to Qinglong: `ss -tnp | grep :5700 > /tmp/qinglong_connections_$(date +%s).txt`. Run `who` and `last -20` to document any active sessions. Collect the Qinglong access log (typically at `/ql/data/log/` or `/root/ql/data/log/`) covering February 7, 2026 onward, preserving file modification timestamps with `stat`. Capture current process tree: `ps auxf > /tmp/process_snapshot_$(date +%s).txt`. These artifacts establish the pre-containment attack surface and active session state before isolation destroys live forensic value.

Step 2: Detection — Review web server and application logs for unauthenticated requests to Qinglong admin endpoints dated on or after February 7, 2026. Look for anomalous process spawning from the Qinglong service account, unexpected outbound connections, and processes masquerading as system services (T1036.005). Check CPU and resource utilization for sustained spikes consistent with cryptomining (T1496).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate log evidence across multiple sources to determine scope of exploitation, identify initial access vector, and assess whether the auth bypass (CVE-2026-3965, CVE-2026-4047) resulted in cryptominer deployment.

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Parse Qinglong application logs with: `grep -E '(GET|POST) /(api|open|manage)' /root/ql/data/log/qinglong.log | grep -v '"Authorization"' | awk '{print $1,$2,$7,$9}' | sort | uniq -c | sort -rn` to surface unauthenticated hits against admin API routes. For anomalous child process detection without EDR, deploy Sysmon (Linux via sysmon-for-linux or Windows equivalent) with a config filtering on ProcessCreate where ParentImage matches the Qinglong Node.js process (typically `node`): look for child processes `curl`, `wget`, `bash`, `sh`, `chmod`, `crontab` spawned by the Qinglong service UID. Use `auditd` rule: `auditctl -a always,exit -F arch=b64 -S execve -F uid= -k qinglong_exec` and review with `ausearch -k qinglong_exec --start 02/07/2026`. For CPU spike correlation: `sar -u 1 10` or review `/proc//stat` for processes consuming >80% CPU with no recognized name — cross-reference against known miner binary hashes using ClamAV with an updated XMRig/cryptominer signature database.

Evidence: Collect: (1) Qinglong application log `/root/ql/data/log/qinglong.log` — grep for HTTP 200 responses to `/api/user/login` or `/open/auth/token` endpoints without valid credential payloads, indicating auth bypass exploitation of CVE-2026-3965/CVE-2026-4047. (2) Linux auth log `/var/log/auth.log` or `/var/log/secure` for the Qinglong service account executing `su`, `sudo`, or spawning shells post-February 7, 2026. (3) Crontab entries for the Qinglong service user: `crontab -u -l` and `/var/spool/cron/crontabs/` — cryptominer persistence via cron is the primary T1053.003 artifact for this campaign. (4) `/tmp`, `/dev/shm`, and `/root/ql/data/scripts/` for dropped ELF binaries with executable bit and no package manager provenance — run `find /tmp /dev/shm /root/ql -type f -executable -newer /root/ql/data/log/qinglong.log -ls`. (5) Outbound network connections to mining pool ports (3333, 4444, 5555, 14444, 45700): `ss -tnp | grep -E ':3333|:4444|:5555|:14444|:45700'`.

Step 3: Eradication — Apply PR #2941 to all Qinglong instances. Confirm the running version is patched beyond 2.20.1. If compromise is confirmed, treat the host as fully compromised: terminate the cryptominer process, terminate the cryptominer process, remove dropped binaries, and audit cron jobs and scheduled tasks for persistence mechanisms.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove all threat artifacts from the environment, remediate the root vulnerability (CVE-2026-3965, CVE-2026-4047 via PR #2941), and verify no persistence mechanisms survive before proceeding to recovery.

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-6 (Configuration Settings), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: To apply PR #2941 on a self-hosted Qinglong instance: `cd /root/ql && git fetch origin && git log origin/main --oneline | head -5` to confirm PR #2941 is merged, then `git pull origin main && pm2 restart qinglong` (or `docker pull whyour/qinglong:latest && docker-compose up -d` for container deployments). Verify the patched version: `curl -s http://localhost:5700/api/public/config | python3 -m json.tool | grep version` — confirm the reported version exceeds 2.20.1. For cryptominer removal without EDR: identify the miner PID via `ps auxf | grep -E '(xmrig|minerd|cryptonight|kswapd0|kworker[^/])' `, kill it with `kill -9 `, then locate the binary with `ls -la /proc//exe` BEFORE killing (this symlink resolves to the actual binary path). Remove with `rm -f `. Enumerate all cron persistence: `for user in $(cut -f1 -d: /etc/passwd); do crontab -u $user -l 2>/dev/null | grep -v '^#' && echo "--- $user"; done`. Remove any entries referencing unknown scripts or base64-encoded commands. Check systemd timers: `systemctl list-timers --all | grep -v systemd`.

Evidence: BEFORE eradication, forensically preserve: (1) A full memory dump of the running cryptominer process using `gcore ` or `procdump` — this captures the miner config including pool address, wallet address, and worker ID attributable to this campaign. (2) Hash all dropped binaries before deletion: `sha256sum > /tmp/ioc_hashes.txt` — submit to VirusTotal offline via API for campaign correlation. (3) Copy (do not move) all modified crontab files and `/etc/cron.*` directories to an evidence folder with timestamps preserved: `cp -a /var/spool/cron /tmp/evidence/cron_$(date +%s)`. (4) Capture the Qinglong scripts directory state: `find /root/ql/data/scripts/ -type f

-newer /root/ql/package.json -exec ls -la {} \;` — attacker-injected tasks via the auth bypass would appear here as recently modified `.js` or `.sh` files. (5) Document the exact Qinglong version string and git commit hash before patching: `cd /root/ql && git log --oneline -1`.

Step 4: Recovery — After applying PR #2941, verify Qinglong admin endpoints reject unauthenticated requests. Monitor host resource utilization for 72 hours post-remediation to confirm cryptominer removal. Review outbound network traffic for connections to known mining pool infrastructure.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore Qinglong to verified-clean operational state, confirm vulnerability remediation effectiveness, and validate that no cryptominer reinfection or residual C2 activity persists before returning to production.

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CA-7 (Continuous Monitoring), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Validate that PR #2941 successfully closes the auth bypass by replaying a benign unauthenticated probe against the Qinglong API: `curl -v -X GET http://localhost:5700/api/user/profile` — a patched instance must return HTTP 401 or 403, not a 200 with user data. For 72-hour CPU monitoring without SIEM: deploy a cron-based resource logger — `echo '*/5 * * * * root top -bn1 | head -20 >> /var/log/cpu_monitor.log' >> /etc/cron.d/recovery_monitor` — and alert if any process sustains >70% CPU for three consecutive 5-minute samples. For outbound mining pool connection detection without NDR tooling: run Wireshark/tcpdump targeting known mining pool port ranges: `tcpdump -i eth0 -w /tmp/recovery_pcap_$(date +%s).pcap 'tcp and (port 3333 or port 4444 or port 5555 or port 14444 or port 45700)'` in a 30-minute rolling capture reviewed twice daily. Cross-reference resolved hostnames against the Emerging Threats mining pool blocklist using: `tcpdump -A -i eth0 port 3333 | grep -oE '[a-z0-9.-]+\.(com|net|org|io)' | sort -u`.

Evidence: During recovery monitoring, preserve: (1) API response captures from the post-patch unauthenticated probe attempts as proof of remediation effectiveness for audit trail (save `curl -v` output with timestamps). (2) CPU/process logs from the 72-hour monitoring window — specifically any process that appears, runs at high CPU, and then disappears, which would indicate a surviving dropper re-fetching the miner binary. (3) DNS query logs from the host (`/var/log/syslog` grep for `systemd-resolved` or `dnsmasq` entries) for queries to mining pool domains or newly registered domains consistent with miner C2 infrastructure. (4) File integrity check output: run `aide --check` or `tripwire --check` (or manually: `find /root/ql /tmp /dev/shm /usr/local/bin -newer /tmp/patch_timestamp -type f -ls`) to detect any new binaries dropped post-patch, which would indicate a separate persistence mechanism surviving eradication.

Step 5: Post-Incident — Assess why Qinglong panels were internet-exposed without authentication controls or network segmentation. Review the asset inventory process for open-source scheduler and admin panel exposure. Implement a policy requiring all admin panels to sit behind VPN or IP allowlisting regardless of application-layer auth.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons learned to identify the organizational control gaps (asset visibility, network segmentation policy, open-source component governance) that permitted Qinglong port 5700 to be internet-exposed without compensating controls, and update policies to prevent recurrence across all admin panel deployments.

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), NIST CM-8 (System Component Inventory), NIST SC-7 (Boundary Protection), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For asset discovery of exposed admin panels without enterprise tooling: run a weekly internal scan using `nmap -p 5700,8080,9000,3000,8443 --open -oG - 10.0.0.0/8 | grep 'open' > /var/log/weekly_admin_panel_scan.txt` to identify any newly exposed scheduler or admin interfaces. For open-source

component inventory, parse all `package.json`, `requirements.txt`, and `docker-compose.yml` files across the environment: `find / -name 'package.json' -not -path '*/node_modules/*' -exec grep -l 'qinglong\|task-scheduler' {} \;`. Implement a VPN-or-allowlist policy enforcement check using a monthly `nmap` scan from an external IP (or use Shodan Monitor free tier on your IP ranges) to detect any admin panel re-exposure. Document findings in a post-incident report that explicitly maps the Qinglong exposure to a gap in CIS 1.1 asset inventory coverage for containerized open-source workloads.

Evidence: For the lessons-learned review, retrieve and preserve: (1) Firewall/perimeter rule history showing when and by whom port 5700 was permitted inbound — this establishes whether the exposure was a misconfiguration, an intentional but undocumented decision, or a gap in change management under NIST CM-3 (Configuration Change Control). (2) The asset inventory records (or absence thereof) for the affected Qinglong host — document whether it appeared in CMDB/inventory at the time of exploitation to quantify the CIS 1.1 gap. (3) Shodan or Censys historical scan data (freely available via their web interfaces) showing when the Qinglong panel on port 5700 first appeared in internet-wide scans relative to the February 7, 2026 exploitation start date — this establishes attacker dwell-time opportunity. (4) Patch notification records: confirm whether CISA KEV or vendor advisories for CVE-2026-3965/CVE-2026-4047 were received and by whom, to assess SI-5 (Security Alerts, Advisories, and Directives) process effectiveness.

Detection Guidance

Primary indicators: unauthenticated HTTP requests to Qinglong admin endpoints in access logs on or after February 7, 2026; anomalous child process creation from the Qinglong Node.js process (e.g., bash, sh, curl, wget spawned by the scheduler service); new binaries written to /tmp, /dev/shm, or world-writable directories; processes with names matching common system daemons (e.g., kworker, sysupdate) that do not match expected system process paths (T1036.005). Behavioral indicators: sustained CPU utilization above baseline on Qinglong hosts; outbound connections to mining pool domains or IPs (typically port 3333, 4444, or 14444); disabled or killed security agents (T1562.001). Log sources to query: application access logs, /var/log/syslog or journald for process creation events, auditd exec logs if enabled, network flow logs for unexpected outbound connections.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`N/A — no specific IOC values confirmed in available sources`	Mining pool connection destinations and dropper hashes not publicly disclosed at time of this report; monitor outbound connections on ports 3333, 4444, 14444 as behavioral indicators	LOW

Framework Mappings

MITRE-ATTACK

- **T1496** — Resource Hijacking
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1562** — Impair Defenses
- **T1105** — Ingress Tool Transfer

- **T1059.004** — Unix Shell
- **T1190** — Exploit Public-Facing Application
- **T1562.001** — Disable or Modify Tools
- **T1036** — Masquerading
- **T1059** — Command and Scripting Interpreter

NIST-800-53R5

- **AC-6** — Least Privilege
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **CM-7** — Least Functionality
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **SI-10** — Information Input Validation
- **AC-3** — Access Enforcement
- **IA-2** — Identification and Authentication (Organizational Users)

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A01:2021** — Broken Access Control

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.1** — Establish an Access Granting Process
- **6.8** — Define and Maintain Role-Based Access Control
- **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

ISO-27001-2022

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

NIST-CSF-2

- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1496	Resource Hijacking	Impact
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1562	Impair Defenses	Defense-Evasion
T1105	Ingress Tool Transfer	Command-And-Control
T1059.004	Unix Shell	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1562.001	Disable or Modify Tools	Defense-Evasion
T1036	Masquerading	Defense-Evasion
T1059	Command and Scripting Interpreter	Execution

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/hackers-exploit-rce-...	T3
CVE-2026-3965 - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-3965	T1
Qinglong RCE Flaws Exploited for Cryptomining	https://snyk.io/blog/qinglong-task-scheduler-rce-vulnerabilities/	T3
CVE Record: CVE-2026-4047	https://www.cve.org/CVERecord?id=CVE-2026-4047	T3
Qinglong RCE Flaws Exploited for Cryptomining	https://app.daily.dev/posts/qinglong-rce-flaws-exploited-for-crypto...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-3965, CVE-2026-4047	T1

DISCLAIMER

Generated 2026-04-30 06:31 UTC by TJS Security Command Center