INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-22 06:47 UTC

CVE-2026-6574: A vulnerability has been found in osuuu LightPicture up to 1.2.2. This issue affects some unknown pr...

CVE VULNERABILITY | HIGH | CVSS 7.3

SCC Item ID	SCC-CVE-2026-0068
Type	CVE Vulnerability
CVE ID	CVE-2026-6574
Severity	HIGH
CVSS Base Score	7.3
EPSS Score	0.0004 (11th percentile)
Affected Products	osuuu LightPicture up to and including version 1.2.2
Published	2026-04-19T14:16:11.593
Discovery Source	Nvd

Executive Summary

A hard-coded credentials vulnerability in osuuu LightPicture (versions up to 1.2.2) allows unauthenticated remote attackers to access protected API functions using credentials embedded in the application's install file. The vendor has not responded to disclosure contact, meaning no official patch exists. Organizations running LightPicture for image hosting or management should treat this as an unpatched, publicly exploitable risk requiring immediate action.

Technical Analysis

CVE-2026-6574 is a hard-coded credentials vulnerability (CWE-259, CWE-798) in osuuu LightPicture up to and including version 1.2.2. The vulnerable credential is embedded in /public/install/lp.sql, within the API Upload Endpoint component. An unauthenticated remote attacker can manipulate the 'key' argument to authenticate using the hard-coded value, potentially gaining unauthorized API access. MITRE ATT&CK techniques T1552.001 (Credentials in Files) and T1078 (Valid Accounts) apply. CVSS base score is 7.3 (High). EPSS score is 0.00038 (0.11th percentile), indicating this vulnerability is exploited less frequently than 99.89% of known vulnerabilities, showing low current exploitation activity in the wild. A public exploit has been disclosed. The vendor did not respond to pre-disclosure contact; no patch is available. Source: NVD (https://nvd.nist.gov/vuln/detail/CVE-2026-6574).

Action Checklist

1. Immediately restrict external access to LightPicture instances running version 1.2.2 or earlier. Block internet-facing exposure at the firewall or reverse proxy layer until remediation is confirmed. Rotate or invalidate any API keys currently in use.
2. Search web server and application logs for unusual POST or authenticated API requests to the Upload Endpoint, particularly requests that authenticated without expected user context. Review /public/install/lp.sql on deployed instances to confirm presence of the hard-coded credential and determine if it has been invoked in access logs.
3. No vendor patch is currently available. Mitigation options: remove or restrict access to /public/install/lp.sql from the web root; disable or firewall the affected API Upload Endpoint; replace LightPicture with a patched alternative if a vendor release becomes available. Monitor the CVE record at https://nvd.nist.gov/vuln/detail/CVE-2026-6574 for patch availability.
4. After applying mitigations, verify /public/install/lp.sql is no longer publicly accessible via HTTP. Confirm API endpoint access controls are functioning. Audit all API access logs retroactively from the deployment date to identify any unauthorized use of the hard-coded credential.
5. This incident exposes a gap in pre-deployment security review of third-party applications. Add hard-coded credential scanning (e.g., via truffleHog, git-secrets, or equivalent) to your software intake and CI/CD review process. Update vendor due diligence procedures to include responsiveness to security disclosure as an evaluation criterion.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if the retroactive log audit (Recovery step) identifies any source IPs external to the organization that authenticated using the hard-coded credential in LightPicture's lp.sql, as this constitutes confirmed unauthorized access to the upload API and may trigger breach notification obligations under applicable data protection regulations if user-uploaded images or associated metadata are in scope.
Recovery Notes	After mitigations are confirmed effective (lp.sql inaccessible via HTTP, Upload Endpoint returning 403), maintain heightened monitoring of LightPicture web server logs for 30 days watching for probing of the former upload endpoint path and any re-emergence of the hard-coded credential username in authentication events. If the retroactive audit identified any unauthorized access, treat all files uploaded to LightPicture during the exposure window as potentially attacker-controlled and audit stored images for web shells or malicious content using `clamscan -r /var/www/lightpicture/uploads/`. Resume full external exposure only after either a vendor patch for CVE-2026-6574 is applied or LightPicture is replaced with a vetted alternative, not on the basis of mitigations alone.

Forensic Artifacts	nginx/Apache access logs (/var/log/nginx/access.log, /var/log/apache2/access.log) — filter for HTTP POST requests to LightPicture's upload and API paths authenticated with the hard-coded credential username extracted from lp.sql; these logs establish the exploitation timeline and attacker source IPs | /public/install/lp.sql — the install SQL file containing the hard-coded credential INSERT statement; preserve SHA-256 hash and exact credential values as the primary indicator of the vulnerability mechanism specific to CVE-2026-6574 | LightPicture application database (MySQL/MariaDB) session and user tables — query for active or historical sessions associated with the hard-coded credential account to determine whether the credential was used to establish persistent authenticated sessions beyond individual API calls | Web root upload directory (/var/www/lightpicture/uploads/ or equivalent) — enumerate all files uploaded during the exposure window sorted by timestamp (`find /var/www/lightpicture/uploads/ -newer /var/www/lightpicture/public/install/lp.sql -type f`) and scan with ClamAV for web shells or malicious payloads deposited via the unprotected Upload Endpoint | Reverse proxy or WAF request logs with Authorization header or session cookie values — if the proxy logs request headers, extract all Authorization values presented to the LightPicture application during the exposure window to identify whether the hard-coded credential was presented from multiple sources, indicating active exploitation rather than opportunistic scanning

Per-Action IR Details

Containment — Immediately restrict external access to LightPicture instances running version 1.2.2 or earlier. Block internet-facing exposure at the firewall or reverse proxy layer until remediation is confirmed. Rotate or invalidate any API keys currently in use.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems to prevent further unauthorized access while preserving evidence for analysis

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: On Linux hosts with nginx or Apache as the reverse proxy, immediately add a deny rule: `sudo ufw deny from any to any port 80,443 comment 'CVE-2026-6574 lockdown'` or insert `deny all` in the nginx `location /` block and reload (`nginx -s reload`). For iptables: `iptables -I INPUT -p tcp --dport 80 -j DROP && iptables -I INPUT -p tcp --dport 443 -j DROP`. Snapshot current API key hashes from LightPicture's database (`SELECT * FROM lp_users`) before rotation so the pre-rotation state is preserved as evidence.

Evidence: Before blocking access, capture: (1) current nginx/Apache access logs in full (`/var/log/nginx/access.log`, `/var/log/apache2/access.log`) — do not rotate or truncate; (2) a read-only copy of `/public/install/lp.sql` to confirm the embedded credential string; (3) LightPicture's application database dump (`mysqldump` or `pg_dump`) to baseline current user and session state; (4) active network connection snapshot (`ss -tnp` or `netstat -tnp`) to identify any live sessions to the LightPicture instance at time of containment.

Detection — Search web server and application logs for unusual POST or authenticated API requests to the Upload Endpoint, particularly requests that authenticated without expected user context. Review /public/install/lp.sql on deployed instances to confirm presence of the hard-coded credential and determine if it has been invoked in access logs.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate log sources to identify indicators of exploitation of the hard-coded credential in LightPicture's install artifact

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Run this grep against nginx/Apache access logs to isolate API authentication events against the Upload Endpoint: `grep -E 'POST.*/upload|POST.*/api' /var/log/nginx/access.log | grep -v '401\|403' > suspicious_upload_requests.txt`. To identify requests authenticated with the hard-coded credential, extract the credential value from `/public/install/lp.sql` (look for INSERT statements into user or admin tables), then search logs for any session tokens or user-agent patterns associated with that credential's user context. Use `jq` if LightPicture emits JSON application logs: `cat app.log | jq 'select(.user == "")'`. For timeline reconstruction, use `goaccess` (free, CLI) on the access log to visualize request volume spikes by endpoint.

Evidence: Capture before analysis: (1) raw web server access logs from deployment date to present, specifically filtering on HTTP POST to the LightPicture upload or API paths; (2) the literal credential value (username and password hash or plaintext) embedded in `/public/install/lp.sql` — document it exactly as it appears; (3) LightPicture session or authentication logs (application-level, if enabled) showing login events correlated against the hard-coded username; (4) any WAF or reverse-proxy authentication logs that record the Authorization header or session cookie values for API calls — these can confirm whether the hard-coded credential was presented in requests from unexpected IPs.

Eradication — No vendor patch is currently available. Mitigation options: remove or restrict access to /public/install/lp.sql from the web root; disable or firewall the affected API Upload Endpoint; replace LightPicture with a patched alternative if a vendor release becomes available. Monitor the CVE record at https://nvd.nist.gov/vuln/detail/CVE-2026-6574 for patch availability.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove the vulnerability mechanism (web-accessible install credential file and unprotected Upload Endpoint) from the environment in the absence of a vendor-supplied patch

Controls: NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Move `/public/install/lp.sql` outside the web root immediately: `mv /var/www/lightpicture/public/install/lp.sql /root/lp_backup_evidence/lp.sql && chmod 600 /root/lp_backup_evidence/lp.sql`. Confirm the file is no longer HTTP-accessible: `curl -o /dev/null -s -w '%{http_code}' http://localhost/public/install/lp.sql` — expected result is 404. Block the Upload Endpoint at the nginx level by adding `location /api/upload { deny all; return 403; }` before the catch-all location block. Set a weekly cron job to monitor the NVD record for CVE-2026-6574 using: `curl -s 'https://services.nvd.nist.gov/rest/json/cves/2.0?cveId=CVE-2026-6574' | jq '.vulnerabilities[0].cve.metrics'` and alert on any change to the remediation field.

Evidence: Before eradication actions, preserve: (1) an SHA-256 hash of `/public/install/lp.sql` (`sha256sum /public/install/lp.sql`) to document the exact credential artifact as evidence; (2) a directory listing and file modification timestamps for the entire `/public/install/` path (`ls -la /var/www/lightpicture/public/install/`) to establish whether the file was modified or accessed post-deployment; (3) web server configuration files (nginx.conf, .htaccess) to document the pre-remediation access control state; (4) a snapshot of the LightPicture application version file or composer.json/package.json to confirm version 1.2.2 or earlier is confirmed in scope.

Recovery — After applying mitigations, verify /public/install/lp.sql is no longer publicly accessible via HTTP. Confirm API endpoint access controls are functioning. Audit all API access logs retroactively from the deployment date to identify any unauthorized use of the hard-coded credential.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore LightPicture to a known-safe operational state, verify mitigations are effective, and confirm no unauthorized access persists via the hard-coded credential

Controls: NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), NIST SI-6 (Security and Privacy Function Verification), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Verify file removal with an external HTTP check from a separate host: `curl -I http:///public/install/lp.sql` — confirm HTTP 403 or 404. Test Upload Endpoint lockdown: `curl -X POST http:///api/upload -H 'Content-Type: application/json'` — confirm HTTP 403. For the retroactive log audit, script a full

sweep: `grep -n '' /var/log/nginx/access.log* | tee retroactive_audit_$(date +%Y%m%d).txt` substituting the actual username extracted from `lp.sql`. Use `awk '{print $1}' retroactive_audit.txt | sort | uniq -c | sort -rn` to identify source IPs that used the hard-coded credential, then cross-reference against expected internal IP ranges.

Evidence: During recovery verification, capture: (1) timestamped curl output confirming 403/404 on `/public/install/lp.sql` — save as `curl_verify_$(date +%Y%m%d_%H%M%S).txt`; (2) the complete retroactive audit output showing every log line where the hard-coded credential username appears, with source IPs and timestamps, spanning from LightPicture deployment date to containment date; (3) a post-mitigation snapshot of the LightPicture user and session database tables to confirm no active sessions remain for the hard-coded credential account; (4) nginx/Apache error logs confirming the Upload Endpoint deny rule is producing 403 responses on test probes.

Post-Incident — This incident exposes a gap in pre-deployment security review of third-party applications. Add hard-coded credential scanning (e.g., via truffleHog, git-secrets, or equivalent) to your software intake and CI/CD review process. Update vendor due diligence procedures to include responsiveness to security disclosure as an evaluation criterion.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: lessons-learned review and process improvement to prevent recurrence of unvetted third-party application deployment with embedded credentials

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SA-11 (Developer Testing and Evaluation), NIST SI-2 (Flaw Remediation), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Integrate `truffleHog` into the software intake process at zero cost: `pip install truffleHog && trufflehog filesystem /path/to/extracted/lightpicture/` — run this against any third-party application archive before deployment and review output for high-entropy strings and known credential patterns. For CI/CD pipelines, add a pre-merge `git-secrets --scan` hook: `git secrets --install && git secrets --register-aws && git secrets --scan-history`. Document a vendor security responsiveness checklist: (1) does the vendor have a published CVD policy or security contact? (2) did the vendor respond within 90 days of disclosure? — failing this check should require CISO sign-off before deployment. Schedule a quarterly scan of all web root directories for `.sql` install files: `find /var/www -name '*.sql' -o -name 'install*' | tee quarterly_install_artifact_scan.txt`.

Evidence: For the lessons-learned record, preserve: (1) the original LightPicture deployment ticket or change record showing whether a pre-deployment security review was required and whether it was performed; (2) the CVE-2026-6574 NVD record and any vendor communication attempts (or lack thereof) to document the no-patch status and vendor non-responsiveness; (3) the retroactive audit results from the Recovery phase showing the full scope of hard-coded credential usage; (4) truffleHog scan output from a post-incident run against the LightPicture installation to document exactly which files contained the credential and serve as a baseline for future scan configuration.

Detection Guidance

Review HTTP access logs for the LightPicture application, specifically for requests to the API Upload Endpoint path. Look for authenticated API requests that do not correspond to known user sessions or expected upload activity. Search application logs for use of the 'key' parameter in API requests. On the host, confirm whether /public/install/lp.sql is accessible from the web root (a direct HTTP GET to that path should return a 403 or 404 in a hardened deployment; a 200 response indicates exposure). No public IOC hashes or IP indicators are currently associated with active exploitation per available sources.

Framework Mappings

MITRE-ATTACK

- **T1552.001** — Credentials In Files
- **T1078** — Valid Accounts

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-12** — Cryptographic Key Establishment and Management

OWASP-TOP10-2021

- **A02:2021** — Cryptographic Failures
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

HIPAA-SECURITY

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

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1552.001	Credentials In Files	Credential-Access
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-6574	T1
CVE Record: CVE-2026-6574 - CNA: VulDB	https://www.cve.org/CVERecord?id=CVE-2026-6574	T3
CVE-2026-6574 | Tenable®	https://www.tenable.com/cve/CVE-2026-6574	T3
CVE-2026-6574 | Mondoo Vulnerability Intelligence	https://mondoo.com/vulnerability-intelligence/vulnerability/CVE-202...	T3
CVE-2026-6574: A vulnerability has been Vulnerability | Sher	https://www.sherlockforensics.com/blog/2026-04-20-cve-2026-6574.html	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. 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 2026-04-22 06:47 UTC by TJS Security Command Center