INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-29 14:02 UTC

CVE-2026-27771: Critical Gitea Container Registry Vulnerability Exposes Private Images to Unauthenticated Attackers

CVE VULNERABILITY | **CRITICAL** | CVSS 9.1

SCC Item ID	SCC-CVE-2026-0238
Type	CVE Vulnerability
CVE ID	CVE-2026-27771
Severity	CRITICAL
CVSS Base Score	9.1
Affected Products	Gitea (built-in container registry, specific version range unconfirmed from available source data)
Published	1 day ago
Discovery Source	Serper

Executive Summary

A critical unauthenticated access vulnerability (CVE-2026-27771, CVSS 9.1) has been publicly disclosed in Gitea's built-in container registry. Any organization running Gitea's container registry may have exposed private container images to unauthorized parties without requiring any credentials. Exposed images frequently contain application source code, API keys, database credentials, and proprietary software, creating direct pathways to broader infrastructure compromise.

Technical Analysis

CVE-2026-27771 affects Gitea's built-in container registry component. The vulnerability is classified under CWE-306 (Missing Authentication for Critical Function), indicating the registry serves private images without enforcing authentication checks. Unauthenticated remote attackers can pull private container images directly. MITRE ATT&CK techniques T1078 (Valid Accounts, bypassed) and T1530 (Data from Cloud Storage) apply. CVSS base score is 9.1 (Critical); CVSS vector is pending NVD publication. EPSS data is not yet available. The CVE is not currently listed on the CISA KEV catalog. Specific affected version ranges and patch versions are unconfirmed from available source data. Initial public disclosure appears in security researcher and news outlets (Orca Security, The Hacker News); NVD entry and official Gitea security advisory should be monitored for vendor-confirmed technical details and affected version ranges. Technical root cause (missing middleware, broken access control logic) is not confirmed from accessible source material. Confidence on technical

specifics: LOW, treat version ranges and patch paths as unverified until NVD, Gitea's official advisory, or CISA confirms them.

Action Checklist

1. Step 1: Containment, Identify all Gitea instances running the built-in container registry. Immediately restrict external network access to the Gitea container registry port (typically 5000/tcp or via reverse proxy path) using firewall rules or WAF policies. If the registry is internet-facing, take it offline or place it behind IP allowlisting until patched. Reference: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection, Query reverse proxy and web server access logs for unauthenticated GET requests to registry API paths (e.g., /v2///manifests/, /v2///blobs/) where no Authorization header is present and HTTP 200 was returned. Check Gitea application logs for container image pull events lacking associated user sessions. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), MITRE D3FEND D3-SFA (System File Analysis).
3. Step 3: Eradication, Apply the official Gitea patch once published on the Gitea releases page (monitor https://github.com/go-gitea/gitea/releases) or the NVD entry (https://nvd.nist.gov/vuln/detail/CVE-2026-27771, patch availability to be confirmed). If no patch is available, disable the container registry feature in Gitea's app.ini ([packages] ENABLED = false) until a fix is confirmed. Rotate any secrets, API keys, or credentials present in images stored in the affected registry. Reference: NIST SI-4 (System Monitoring), CIS 7.3 (Perform Automated Operating System Patch Management), MITRE D3FEND D3-CRO (Credential Rotation).
4. Step 4: Recovery, After patching, verify that unauthenticated requests to registry API endpoints return HTTP 401 or 403. Re-enable registry access incrementally, starting with internal-only access before restoring external exposure. Enable authentication logging and confirm AU-3-compliant audit records (who, what, when, where) are being captured for all registry pull events. Reference: NIST AU-3 (Content of Audit Records), NIST AC-3 (Access Enforcement), MITRE D3FEND D3-LAM (Local Account Monitoring).
5. Step 5: Post-Incident, Conduct a review of all container images stored in the affected registry to catalog what sensitive data (secrets, credentials, source code) was present. Implement a secrets scanning step in your CI/CD pipeline to prevent credentials from being baked into images going forward. Review access control policies for all developer-facing infrastructure under NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges). Evaluate whether any exposed secrets require enterprise-wide credential rotation under MITRE D3FEND D3-CH (Credential Hardening).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if access log analysis (Step 2) confirms any HTTP 200 responses to unauthenticated /v2/ registry API requests, as this constitutes confirmed data exposure of container image contents and may trigger breach notification obligations if those images contained PII, PHI, credentials to systems processing regulated data, or customer-identifiable source code.

Recovery Notes	After patching and verifying HTTP 401 responses on unauthenticated registry probes, monitor Gitea application logs and reverse proxy access logs daily for a minimum of 30 days for anomalous pull activity — specifically any authenticated pulls from IPs that previously appeared in the unauthenticated access log window, which may indicate an attacker returning with credentials extracted from exposed images. Re-image any container workloads whose runtime images were stored in the affected registry and could not be conclusively cleared of embedded secrets via layer analysis. Confirm all rotated credentials (API keys, DB passwords, service account tokens found in image layers) have been invalidated at the source system before closing the incident.
Forensic Artifacts	Nginx/Apache/Caddy reverse proxy access logs: entries matching `GET /v2///(manifests|blobs)/` with HTTP 200 response code and absent Authorization request header — these are the direct evidence of unauthenticated image pulls via CVE-2026-27771 | Gitea application log (`ROOT_PATH` per app.ini `[log]` section): package and container pull events lacking an authenticated user session identifier — corroborates proxy logs and identifies which specific image tags were accessed | Gitea database export of the `package` and `package_version` tables (SQLite: `.dump package`, PostgreSQL: `pg_dump -t package -t package_version gitea`): provides the authoritative inventory of every container image namespace, name, tag, and upload timestamp that was stored and potentially exposed | Container image layer tarballs extracted via `crane export` for each image in the registry: the actual forensic content showing what source code, configuration files, and embedded secrets were present in the layers accessible to unauthenticated requestors during the exposure window | Network flow or firewall logs for port 5000/tcp (or the configured reverse proxy port) covering the period from Gitea instance deployment through containment timestamp: used to identify source IPs and data volume of potential bulk image pulls, supporting both blast radius assessment and threat actor attribution

Per-Action IR Details

Step 1: Containment — Identify all Gitea instances running the built-in container registry. Immediately restrict external network access to the Gitea container registry port (typically 5000/tcp or via reverse proxy path) using firewall rules or WAF policies. If the registry is internet-facing, take it offline or place it behind IP allowlisting until patched. Reference: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers).

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: On Linux hosts: run `sudo ss -tlnp | grep -E '5000|gitea'` to confirm which process is bound to the registry port, then block with `sudo iptables -I INPUT -p tcp --dport 5000 -j DROP && sudo iptables -I INPUT -p tcp --dport 3000 -m string --string '/v2/' --algo bm -j DROP`. For reverse-proxy setups (nginx/Caddy), comment out the `/v2/` location block and reload. Document the exact timestamp and approving analyst in a change ticket before executing — this is your containment timestamp for NIST 800-61r3 §3.3 evidence chain.

Evidence: Before restricting access, snapshot current network state: capture `sudo netstat -antp | grep gitea` output, export current iptables/nftables ruleset (`iptables-save > pre-containment-$(date +%F).rules`), and preserve the Gitea `app.ini` configuration file (typically `/etc/gitea/app.ini` or `/opt/gitea/custom/conf/app.ini`) showing `[packages] ENABLED = true` as confirmation the registry feature was active. This establishes the pre-remediation baseline and scope of exposure for the incident record.

Step 2: Detection — Query reverse proxy and web server access logs for unauthenticated GET requests to registry API paths (e.g., /v2///manifests/, /v2///blobs/) where no Authorization header is present and HTTP 200

was returned. Check Gitea application logs for container image pull events lacking associated user sessions. Reference: NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs), MITRE D3FEND D3-SFA (System File Analysis).

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-3 (Content of Audit Records), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Parse nginx or Apache access logs with: `grep -E 'GET /v2/.+/(manifests|blobs)' /var/log/nginx/access.log | grep -v 'Authorization' | awk '{print $1, $7, $9}' | sort | uniq -c | sort -rn`. For Gitea's own application log (default path `/var/log/gitea/gitea.log` or as configured in `app.ini` under `[log] ROOT_PATH`), search for `packages` or `container` pull events: `grep -iE 'container|package|pull|manifest|blob' /var/log/gitea/gitea.log | grep -v 'user='`. Any HTTP 200 response to `/v2/` paths without a corresponding authenticated session ID is a confirmed unauthorized pull. For timeline correlation, use `awk` to bucket hits by hour to identify bulk exfiltration windows.

Evidence: Preserve the following before log rotation occurs: (1) Full nginx/Apache/Caddy access logs covering at minimum 90 days prior to CVE disclosure date — specifically entries matching `GET /v2/` with HTTP 200 responses and no `Authorization:` header in request; (2) Gitea application log showing package/container access events — located per `[log] ROOT_PATH` in `app.ini`; (3) A complete list of all container image namespaces and tags stored in the registry, exported via `gitea admin` CLI or direct query of the Gitea database (`SELECT * FROM package WHERE type='container'` against the configured SQLite/PostgreSQL/MySQL backend) — this inventory is required to scope what was exposed.

Step 3: Eradication — Apply the official Gitea patch once confirmed via the Gitea releases page (https://github.com/go-gitea/gitea/releases) or the NVD entry for CVE-2026-27771 (https://nvd.nist.gov/vuln/detail/CVE-2026-27771). If no patch is available, disable the container registry feature in Gitea's app.ini ([packages] ENABLED = false) until a fix is confirmed. Rotate any secrets, API keys, or credentials present in images stored in the affected registry. Reference: NIST SI-4 (System Monitoring), CIS 7.3 (Perform Automated Operating System Patch Management), MITRE D3FEND D3-CRO (Credential Rotation).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.2 (Use Unique Passwords)

Compensating: If a patch is not yet released, set `[packages] ENABLED = false` in `app.ini` and restart Gitea (`sudo systemctl restart gitea`), then confirm the registry is unreachable: `curl -sk https:///v2/ -o /dev/null -w '%{http_code}'` — expected result is 404 or connection refused. For secret rotation, extract image layers locally using `crane` (free: `go install github.com/google/go-containerregistry/cmd/crane@latest`) and scan each layer with `trufflehog filesystem ` (free, open source) to enumerate every credential that must be rotated. Document each rotated secret with rotation timestamp for the incident record.

Evidence: Before patching, capture the Gitea binary hash for version confirmation: `sha256sum $(which gitea)`. After patching, capture the new binary hash and the patched version string (`gitea --version`) to record in the change log. For each container image identified as exposed, pull and inspect the full layer history using `crane export : - | tar -tv` to document what file contents (and therefore what secrets or source code) were accessible to unauthenticated requestors — this output is the blast radius evidence required for breach notification analysis.

Step 4: Recovery — After patching, verify that unauthenticated requests to registry API endpoints return HTTP 401 or 403. Re-enable registry access incrementally, starting with internal-only access before restoring external exposure. Enable authentication logging and confirm AU-3-compliant audit records (who, what, when, where) are being captured for all registry pull events. Reference: NIST AU-3 (Content of Audit Records), NIST AC-3 (Access Enforcement), MITRE D3FEND D3-LAM (Local Account Monitoring).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-3 (Content of Audit Records), NIST AC-3 (Access Enforcement), NIST AC-4 (Information Flow Enforcement), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Verify the fix with three targeted curl probes before restoring any access: (1) unauthenticated manifest fetch: `curl -sk -o /dev/null -w '%{http_code}' https:///v2///manifests/latest` — must return 401; (2) unauthenticated blob fetch: `curl -sk -o /dev/null -w '%{http_code}' 'https:///v2///blobs/` — must return 401; (3) authenticated fetch with valid token to confirm legitimate access still works. Restore internal access only after all three probes pass. Set up a daily cron job: `curl -sk -o /dev/null -w '%{http_code}' https:///v2///manifests/latest >> /var/log/gitea-auth-check.log` to catch regression.

Evidence: Capture and archive the verification probe outputs with timestamps as evidence of confirmed remediation. Pull a sample of Gitea application logs post-patch and confirm each registry access event contains: authenticated user identity, source IP, image name and tag, and timestamp — these are the AU-3 fields required for the incident record. If log entries still lack user identity fields after patching, escalate to the Gitea maintainer — incomplete audit records must be noted as a residual risk in the post-incident report.

Step 5: Post-Incident — Conduct a review of all container images stored in the affected registry to catalog what sensitive data (secrets, credentials, source code) was present. Implement a secrets scanning step in your CI/CD pipeline to prevent credentials from being baked into images going forward. Review access control policies for all developer-facing infrastructure under NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges). Evaluate whether any exposed secrets require enterprise-wide credential rotation under MITRE D3FEND D3-CH (Credential Hardening).

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST RA-3 (Risk Assessment), NIST AU-11 (Audit Record Retention), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 3.2 (Establish and Maintain a Data Inventory)

Compensating: Run `trufflehog image :` against every image in the Gitea registry inventory to produce a secrets exposure report — output to a timestamped file per image. For CI/CD pipeline hardening without commercial tooling, add a `trufflehog git` pre-commit hook and a `docker build` post-step that runs `trufflehog image` on the newly built image before push, failing the pipeline on any high-confidence finding. To enforce least privilege on Gitea itself, audit all Gitea user accounts with admin or owner roles: `gitea admin user list` and cross-reference against your access inventory from CIS 5.1 — remove any accounts that don't require registry write access.

Evidence: Retain the following for the post-incident record and any required breach notification: (1) The full container image inventory with per-image secrets scan output from trufflehog, documenting exactly what credential classes were present in exposed images; (2) The access log extracts from Step 2 showing confirmed unauthorized pulls, with source IPs and timestamps — this is the evidence set for determining notification obligations if the exposed images contained customer data or regulated information; (3) The pre- and post-patch Gitea binary hashes from Step 3; (4) All credential rotation records with timestamps, mapping each rotated secret back to the image layer it was found in. Retain this package per your AU-11 retention schedule.

Detection Guidance

Focus detection on Gitea container registry API endpoints. Query access logs (nginx, Apache, Gitea application logs) for HTTP GET requests to paths matching /v2/*/manifests/* and /v2/*/blobs/* that returned HTTP 200 without an Authorization request header. Flag any such responses as unauthorized successful pulls. In SIEM environments, create a rule: source_path contains '/v2/' AND http_method = 'GET' AND http_status = 200 AND authorization_header IS NULL. Additionally, review Gitea's package/registry audit logs for pull events with no

associated authenticated user. Behavioral indicator: sustained or bulk pull activity from external IPs against private image namespaces. No confirmed IOCs (hashes, IPs, domains) are currently available from public disclosures. Monitor CISA, security vendor reports, and threat intelligence feeds for IOCs as affected organizations report incidents. Reference NIST AU-6 and CIS 8.2. Apply MITRE D3FEND D3-SFA (System File Analysis) for log integrity checks.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage

NIST-800-53R5

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

OWASP-TOP10-2021

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

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection

Sources

Source	URL	Tier
	https://www.rescana.com/post/cve-2026-27771-critical-gitea-containe...	T3
Gitea Container Registry Flaw - Orca Security	https://orca.security/resources/blog/gitea-container-registry-vulne...	T3
Gitea Vulnerability Exposes Private Container Images without ...	https://thehackernews.com/2026/05/gitea-vulnerability-exposes-priva...	T3
CVE-2026-27771 — Gitea's private container registry served images ...	https://www.reddit.com/r/Gitea/comments/1tpyjwu/cve202627771_giteas...	T3
Gitea flaw exposes private container images without authentication ...	https://www.facebook.com/thehackernews/posts/-gitea-flaw-exposes-pr...	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-27771	T1

Generated 2026-05-29 14:02 UTC by TJS Security Command Center