INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-11 07:44 UTC

Oracle Security Alert: CVE-2026-35273 Affects PeopleSoft Enterprise PeopleTools

CVE VULNERABILITY | HIGH

SCC Item ID	SCC-CVE-2026-0292
Type	CVE Vulnerability
CVE ID	CVE-2026-35273
Severity	HIGH
Affected Products	Oracle PeopleSoft Enterprise PeopleTools (specific versions not confirmed from available data)
Published	6 hours ago
Discovery Source	Serper

Executive Summary

Oracle has issued a standalone Security Alert for CVE-2026-35273 affecting PeopleSoft Enterprise PeopleTools, the foundational platform underpinning Oracle PeopleSoft HR, finance, and ERP deployments. Oracle reserves out-of-cycle Security Alerts for vulnerabilities of elevated severity or active exploitation risk, making this advisory higher priority than a routine quarterly CPU release. Organizations running PeopleSoft in production should treat this as urgent until full technical parameters are confirmed from Oracle's advisory.

Technical Analysis

CVE-2026-35273 affects Oracle PeopleSoft Enterprise PeopleTools. Oracle published a dedicated out-of-cycle Security Alert, a practice Oracle reserves for vulnerabilities of elevated severity or suspected active exploitation, distinguishing this from standard quarterly Critical Patch Update (CPU) advisories. Technical parameters including CVSS base score, attack vector, authentication requirements, CWE classification, and affected version ranges were not available in the source data at time of publishing. Security teams should retrieve current technical details directly from Oracle's advisory at oracle.com/security-alerts/alert-cve-2026-35273.html and NVD (nvd.nist.gov/vuln/detail/CVE-2026-35273) before scoping response. A GitHub Security Advisory (GHSA-25mw-359m-f6rj) is also available. PeopleTools serves as the runtime and development platform for PeopleSoft applications; a vulnerability at this layer can affect the full application stack. CISA KEV inclusion: not confirmed. EPSS score: not available from provided data.

Action Checklist

1. Step 1: Containment, Immediately retrieve Oracle's official Security Alert at oracle.com/security-alerts/alert-cve-2026-35273.html to confirm affected PeopleTools version ranges. Until patch status is confirmed, restrict external network access to PeopleSoft application servers and PIA (PeopleSoft Internet Architecture) endpoints. Apply network-layer access controls limiting PeopleSoft access to trusted internal IP ranges where operationally feasible. Reference: NIST SI-4 (System Monitoring) for active restriction and monitoring of exposed services.
2. Step 2: Detection, Audit your asset inventory (CIS 1.1, Establish and Maintain Detailed Enterprise Asset Inventory) to identify all PeopleSoft PeopleTools deployments and their current version levels. Query your SIEM for anomalous authentication events, unexpected administrative actions, or unusual API calls against PeopleSoft application servers. Enable enhanced logging on PeopleSoft web server and application server tiers per NIST AU-2 (Event Logging) and AU-12 (Audit Record Generation). Cross-reference NVD (nvd.nist.gov/vuln/detail/CVE-2026-35273) for IOC patterns once full technical parameters are published.
3. Step 3: Eradication, Apply Oracle's prescribed patch or mitigation from the official Security Alert advisory immediately upon confirmation of affected versions. Follow Oracle's CPU/Security Alert patching guidance for PeopleTools version upgrade path. Reference NIST SI-2 (Flaw Remediation) and CIS 7.4 (Perform Automated Application Patch Management) for patch management process. Do not apply workarounds from unofficial sources; use only Oracle-published remediation steps.
4. Step 4: Recovery, After patching, validate PeopleTools version strings against Oracle's confirmed fixed-version list. Re-enable any externally facing PeopleSoft services that were restricted during containment only after patch verification. Monitor authentication logs, application server logs, and database audit logs for 72 hours post-remediation per NIST AU-6 (Audit Record Review, Analysis, and Reporting) to confirm no residual malicious activity. Restore network access controls to baseline only after clean monitoring period.
5. Step 5: Post-Incident, Review the organization's Oracle CPU subscription and Security Alert monitoring process; out-of-cycle alerts require a faster detection-to-action pipeline than quarterly CPU cadence. Document any gaps in PeopleTools version inventory that delayed response. Map control improvements to NIST SI-5 (Security Alerts, Advisories, and Directives) to ensure Oracle Security Alerts are routed to operational teams within defined SLAs. Update vulnerability management process per CIS 7.1 (Establish and Maintain a Vulnerability Management Process) to explicitly include out-of-cycle vendor alerts.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to CISO and legal/privacy counsel if forensic review of PeopleSoft PSOPRDEFN, PS_AUDIT_ACTN, or PIA access logs reveals unauthorized access to operator accounts, unexpected privilege grants, or data exfiltration indicators from HR or finance modules, as PeopleSoft typically holds PII and financial records subject to GDPR, HIPAA, SOX, or state breach notification requirements.

Recovery Notes	After applying Oracle's prescribed PeopleTools patch, validate the fixed version string via PS_PTVERSION query on every patched instance before re-enabling external PIA access, and verify web server configuration files (web.xml, psconfig.xml) have not been modified outside the Change Assistant patch process. Conduct a 72-hour enhanced monitoring period targeting PeopleSoft authentication logs, APPSRV.LOG Tuxedo service calls, and Oracle DB audit logs for anomalous operator activity, unexpected DDL against PS_ system tables, or new file creation in $PS_HOME. Given PeopleSoft's role as an HR and finance platform, include a targeted review of PSOPRDEFN for unauthorized operator accounts and PS_ROLEUSER for unauthorized role assignments that may have been made during any exploitation window prior to containment.
Forensic Artifacts	PS_PTVERSION table (queried via SQL against PeopleSoft database): authoritative record of exact PeopleTools build number per instance — required to confirm affected version and verify patch success; capture pre- and post-patch outputs with timestamps | PeopleSoft PIA web server access logs ($PS_HOME/webserv//logs/access_log or IIS equivalent): primary record of inbound HTTP requests to PeopleSoft endpoints; exploitation of PeopleTools web-tier vulnerabilities would appear here as anomalous URIs targeting PSIGW, iclientservlet, or signon components, unusual HTTP methods, or large POST bodies to component interfaces \| PeopleSoft Application Server APPSRV.LOG and Tuxedo ULOG ($PS_CFG_HOME/appserv//LOGS/): records all Tuxedo service invocations between PIA web tier and application tier; exploitation of application-server-side PeopleTools vulnerabilities would produce anomalous service call sequences, authentication failures, or unexpected service names not in normal application workflow | PSOPRDEFN and PS_ROLEUSER tables (PeopleSoft database): operator account and role assignment records — a successful PeopleTools exploit enabling privilege escalation or unauthorized access would leave evidence of new operator creation, password changes, or role grants outside normal provisioning windows; query filtered on LASTUPDDTTM covering the incident window | Oracle Database audit trail (DBA_AUDIT_TRAIL or Unified Auditing logs, if enabled): captures DDL and privileged DML against PeopleSoft system tables (PS_* prefix) from the application service account; anomalous schema modifications or bulk SELECT against HR/finance tables (e.g., PS_PERSONAL_DATA, PS_JOB, PS_VOUCHER) during the incident window would indicate data access or exfiltration following exploitation

Per-Action IR Details

Step 1: Containment — Immediately retrieve Oracle's official Security Alert at oracle.com/security-alerts/alert-cve-2026-35273.html to confirm affected PeopleTools version ranges. Until patch status is confirmed, restrict external network access to PeopleSoft application servers and PIA (PeopleSoft Internet Architecture) endpoints. Apply network-layer access controls limiting PeopleSoft access to trusted internal IP ranges where operationally feasible. Reference: NIST SI-4 (System Monitoring) for active restriction and monitoring of exposed services.

NIST Phase: Containment

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

Controls: NIST SI-4 (System Monitoring), NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Block PeopleSoft PIA HTTP/HTTPS ports (typically TCP 80/443 and 8000/8443) at the perimeter firewall using ACLs scoped to trusted internal CIDR ranges. On the PeopleSoft application server host, apply Windows Firewall or iptables rules immediately: on Linux run 'iptables -I INPUT -p tcp --dport 8443 -s -j ACCEPT && iptables -I INPUT -p tcp --dport 8443 -j DROP'. Capture current netstat output ('netstat -antp | grep 8443') before any changes to preserve established-connection state as pre-containment evidence.

Evidence: Before restricting access, snapshot current active network connections to PeopleSoft PIA endpoints using 'netstat -antp' or 'ss -tnp' on application server hosts to capture any in-progress attacker sessions. Export PeopleSoft web server access logs (default path: $PS_HOME/webserv//logs/access_log or IIS logs at C:\inetpub\logs\LogFiles) covering the 72-hour window prior to containment. Capture PeopleSoft Application Server APPSRV.LOG and TUXEDO ULOG for the same window, as exploit attempts against PeopleTools would generate anomalous Tuxedo service call entries. Document current PeopleTools patch level from PeopleTools version table (PS_PTVERSION in the PeopleSoft database) before any patching begins.

Step 2: Detection — Audit your asset inventory (CIS 1.1 — Establish and Maintain Detailed Enterprise Asset Inventory) to identify all PeopleSoft PeopleTools deployments and their current version levels. Query your SIEM for anomalous authentication events, unexpected administrative actions, or unusual API calls against PeopleSoft application servers. Enable enhanced logging on PeopleSoft web server and application server tiers per NIST AU-2 (Event Logging) and AU-12 (Audit Record Generation). Cross-reference NVD (nvd.nist.gov/vuln/detail/CVE-2026-35273) for IOC patterns once full technical parameters are published.

NIST Phase: Detection Analysis

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

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring)

Compensating: Without a SIEM, query the PeopleSoft database directly for version inventory: run 'SELECT VERSION FROM PS_PTVERSION' against each PeopleSoft database instance to enumerate all deployed PeopleTools builds. Parse PeopleSoft PIA web server access logs with grep or PowerShell to surface anomalous URI patterns: 'grep -E "(iclientservlet|PSIGW|signon\.html)" access_log | awk '{print $1,$7,$9}' | sort | uniq -c | sort -rn'. Deploy Sysmon on PeopleSoft Windows application server hosts with Event ID 3 (Network Connection) and Event ID 1 (Process Creation) to catch unexpected child processes spawned by the PeopleSoft application server service account. Use Wireshark or tcpdump on the PIA network segment to capture and inspect HTTP request bodies to PeopleSoft endpoints for anomalous payloads.

Evidence: Query PS_PTVERSION table across all PeopleSoft database instances to establish exact PeopleTools build numbers before any patching — this is the authoritative version record for affected-version determination. Review PeopleSoft PIA web server access logs for unusual HTTP methods (PUT, DELETE, OPTIONS) or unexpected URIs targeting PeopleSoft Integration Broker (PSIGW servlet) or component interfaces, as these are common attack surfaces in PeopleTools vulnerabilities. Inspect PeopleSoft Application Server APPSRV.LOG for failed or anomalous Tuxedo service invocations, which would indicate exploitation attempts against application-tier components. Check Oracle database audit logs (if DB auditing is enabled) for unexpected DDL or DML against PeopleSoft system tables (PS_* prefix) from the application service account outside normal batch windows.

Step 3: Eradication — Apply Oracle's prescribed patch or mitigation from the official Security Alert advisory immediately upon confirmation of affected versions. Follow Oracle's CPU/Security Alert patching guidance for PeopleTools version upgrade path. Reference NIST SI-2 (Flaw Remediation) and CIS 7.4 (Perform Automated Application Patch Management) for patch management process. Do not apply workarounds from unofficial sources; use only Oracle-published remediation steps.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), CIS 7.4 (Perform Automated Application Patch Management), CIS 7.2 (Establish and Maintain a Remediation Process), NIST IR-4 (Incident Handling)

Compensating: PeopleSoft patching requires Oracle's Change Assistant tool — there is no free-tool substitute for the patch application itself. However, a 2-person team can validate patch integrity before deployment by verifying the SHA-256 checksum of downloaded patch bundles against Oracle's published hash in the advisory (use 'certutil -hashfile SHA256' on Windows or 'sha256sum ' on Linux). After applying the PeopleTools patch via Change Assistant, confirm the updated version string by re-querying 'SELECT VERSION FROM PS_PTVERSION' and comparing against Oracle's fixed-version list from the advisory. Document the exact patch bundle name, application timestamp, and Change Assistant log path as eradication evidence.

Evidence: Before applying the patch, capture a full file listing with timestamps from the PeopleTools installation directory ($PS_HOME on Linux or %PS_HOME% on Windows) using 'find $PS_HOME -newer /tmp/baseline_timestamp -ls' or PowerShell 'Get-ChildItem -Recurse $env:PS_HOME | Select FullName,LastWriteTime' to establish a pre-patch file integrity baseline. Preserve the Change Assistant log from the patch application (typically located at $PS_CFG_HOME/log/ChangeAssistant) as forensic evidence of eradication action. Re-query PS_PTVERSION post-patch and record the output with timestamp as the eradication verification record.

Step 4: Recovery — After patching, validate PeopleTools version strings against Oracle's confirmed fixed-version list. Re-enable any externally facing PeopleSoft services that were restricted during containment only after patch verification. Monitor authentication logs, application server logs, and database audit logs for 72 hours post-remediation per NIST AU-6 (Audit Record Review, Analysis, and Reporting) to confirm no residual malicious activity. Restore network access controls to baseline only after clean monitoring period.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-7 (Software, Firmware, And Information Integrity), NIST IR-5 (Incident Monitoring)

Compensating: Without a SIEM for 72-hour post-patch monitoring, configure a cron job or Windows Scheduled Task to run every 15 minutes parsing PeopleSoft PIA access logs for anomalous response codes (500-series errors or unexpected 302 redirects to non-PeopleSoft domains): 'grep -E " 5[0-9]{2} | 302 " access_log | tail -100'. Monitor PeopleSoft Operator Activity via the delivered PSAUDIT record — query 'SELECT OPRID, LASTLOGINDT, LASTLOGINDTTM FROM PSOPRDEFN WHERE LASTLOGINDTTM > SYSDATE - 3' against the PeopleSoft database every few hours to surface any accounts that authenticated during or after the incident window. Use Sysmon Event ID 11 (File Creation) on application server hosts to detect any new files written to $PS_HOME post-patch that could indicate residual webshell or persistence.

Evidence: During the 72-hour post-patch monitoring window, continuously collect PeopleSoft PIA access logs, APPSRV.LOG, and Oracle database audit logs. Specifically query PSOPRDEFN and PS_AUDIT_ACTN tables in the PeopleSoft database for any privilege escalation events or new operator records created during the incident window — a successful exploit of PeopleTools may enable unauthorized operator account creation or role assignment. Verify integrity of PeopleSoft web server configuration files (web.xml, psconfig.xml under $PS_CFG_HOME/webserv//applications/peoplesoft/PORTAL.war/WEB-INF) by comparing file hashes against the post-patch Change Assistant baseline to detect any implanted modifications.

Step 5: Post-Incident — Review the organization's Oracle CPU subscription and Security Alert monitoring process; out-of-cycle alerts require a faster detection-to-action pipeline than quarterly CPU cadence. Document any gaps in PeopleTools version inventory that delayed response. Map control improvements to NIST SI-5 (Security Alerts, Advisories, and Directives) to ensure Oracle Security Alerts are routed to operational teams within defined SLAs. Update vulnerability management process per CIS 7.1 (Establish and Maintain a Vulnerability Management Process) to explicitly include out-of-cycle vendor alerts.

NIST Phase: Post Incident

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

Controls: NIST SI-5 (Security Alerts, Advisories, And Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), NIST IR-8 (Incident Response Plan), CIS 2.2 (Ensure Authorized Software is Currently Supported), NIST IR-6 (Incident Reporting)

Compensating: Subscribe to Oracle Security Alerts via the Oracle Technology Network mailing list (no-cost) and create a dedicated email rule or ticketing system trigger to auto-escalate any message containing 'Security Alert' (as distinct from quarterly 'Critical Patch Update') to the security operations team within 4 hours of receipt. Build a lightweight PeopleTools version inventory script that queries PS_PTVERSION across all PeopleSoft database instances on a weekly schedule and exports results to a shared CSV — a 2-person team can maintain this with a simple cron job and a read-only DB service account, satisfying CIS 1.1 for PeopleSoft assets without enterprise tooling.

Evidence: Document the timeline delta between Oracle's Security Alert publication date and the organization's first internal awareness as the primary process gap metric for the lessons-learned report. Preserve the PS_PTVERSION query results captured at the start of this incident as evidence of the pre-patch version inventory state, which validates whether the version gap assessment was accurate and supports any regulatory notification decisions. Archive all APPSRV.LOG, PIA access logs, and database audit logs from the incident window in write-protected storage per NIST AU-11 (Audit Record Retention) for post-incident review and potential regulatory inquiry given PeopleSoft's typical role as an HR and finance system of record holding PII.

Detection Guidance

Specific IOC patterns and behavioral indicators for CVE-2026-35273 cannot be confirmed from the available source data; the attack vector, authentication requirement, and technical root cause were not populated in the provided fields. Security teams should retrieve detection signatures from Oracle's advisory and NVD once fully published. In the interim, apply the following general PeopleTools monitoring posture: review PeopleSoft web server access logs for unexpected URIs, parameter tampering patterns, or high-volume requests against PIA endpoints; audit PeopleSoft security logs (PS_AUDIT tables and application server logs) for privilege escalation or unauthorized configuration changes; enable system-level logging per NIST AU-2 and AU-12 across PeopleTools application, web, and database tiers; and monitor for unauthorized changes to PeopleTools configuration files using NIST SI-7 (Software, Firmware, and Information Integrity) or file integrity monitoring (FIM) tools. Subscribe to Oracle Security Alerts RSS feed and CISA Known Exploited Vulnerabilities catalog (cisa.gov/known-exploited-vulnerabilities-catalog) for updated IOC publications.

Framework Mappings

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **8.2** — Collect Audit Logs

ISO-27001-2022

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

NIST-800-53R5

- **SI-4** — System Monitoring
- **IR-5** — Incident Monitoring

NIST-CSF-2

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

Sources

Source	URL	Tier
	https://blogs.oracle.com/security/security-alert-cve-2026-35273-rel...	T3

Source	URL	Tier
Oracle Security Alert Advisory - CVE-2026-35273	https://www.oracle.com/security-alerts/alert-cve-2026-35273.html	T3
CVE-2026-35273 | Tenable®	https://www.tenable.com/cve/CVE-2026-35273	T3
CVE-2026-35273 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-35273	T1
Vulnerability in the PeopleSoft Enterprise PeopleTools... · CVE-2026 ...	https://github.com/advisories/GHSA-25mw-359m-f6rj	T3

Generated 2026-06-11 07:44 UTC by TJS Security Command Center