INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-10 19:20 UTC

ShinyHunters Actively Exploiting Oracle PeopleSoft via Zero-Day Vulnerability Chain, 100+ Organizations Breached

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0437
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Oracle PeopleSoft (cloud and on-premises instances; specific versions not yet publicly confirmed)
Published	2026-06-10T14:31:57
Discovery Source	Rss

Executive Summary

ShinyHunters, a financially motivated extortion group, claims to be actively exploiting a reported vulnerability chain in Oracle PeopleSoft to steal data and demand ransom. The group reports approximately 300 instances across more than 100 organizations compromised; independent verification of this claim is pending. Affected data includes HR records, payroll, finance, and student information. No Oracle patch or official advisory exists as of this report, leaving all unmitigated PeopleSoft deployments at elevated risk while the campaign remains active.

Technical Analysis

ShinyHunters is conducting an active campaign against Oracle PeopleSoft (cloud and on-premises) using a reported vulnerability chain combining previously known weaknesses with claimed zero-days. No CVE has been officially published for the primary zero-day component; CVSS scoring has not been independently verified via NVD. A related NVD entry, CVE-2025-30747, was surfaced during research but its direct relationship to this campaign is unconfirmed; do not treat it as causally linked without further verification. Reported weakness classes are CWE-798 (hardcoded credentials), CWE-287 (improper authentication), and CWE-94 (code injection). Exposed attacker infrastructure includes credential spraying scripts (consistent with T1110.001, T1110.003), ransom note deployment tooling (T1486), lateral movement capabilities (T1021, T1021.004), and ingress tooling (T1105). Additional mapped techniques include T1078/T1078.001 (valid accounts, default accounts), T1190 (exploit public-facing application), T1059/T1059.004 (command execution), T1133 (external

remote services), T1136 (account creation), T1657 (financial extortion), and T1071.002 (application layer protocol: file transfer). No Oracle patch is available. Specific affected PeopleSoft versions have not been publicly confirmed.

Action Checklist

1. Step 1: Containment. Immediately restrict external access to PeopleSoft web-facing components (PIA, Integration Broker endpoints) at the network perimeter. Apply IP allowlisting or take internet-facing PeopleSoft instances offline if business operations permit. No Oracle patch is available; network isolation is the primary containment control until one is released. Reference: NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers).
2. Step 2: Detection. Review authentication logs for credential spraying patterns: more than 5 failed logons against PeopleSoft PIA login endpoints from a single source IP within 10 minutes, followed by successful logon from the same or related source IPs (NIST AU-6, AU-2). Hunt for anomalous shell execution or script invocation from PeopleSoft application server processes. Check for new local or application accounts created outside your provisioning process (CIS 5.1, NIST AC-2). Review file transfer logs and outbound connections for bulk data staging activity. IOCs from exposed attacker infrastructure should be applied to SIEM, firewall, and proxy block lists as they are released by threat intelligence providers. Monitor CISA, Oracle security advisories, and major threat intelligence vendors for published IOC lists. In the interim, prioritize network-layer access controls rather than waiting for IOC lists.
3. Step 3: Eradication. No Oracle patch is available as of this report. Monitor Oracle's Critical Patch Update (CPU) page and security alerts channel for an emergency advisory. In the interim: audit all PeopleSoft accounts and disable or remove accounts not required for operations (CIS 5.3, NIST AC-2); rotate all PeopleSoft service account and administrative credentials immediately (NIST IA-4); audit integration configurations for hardcoded credentials and remediate (NIST IA-5, CWE-798 mitigation); restrict PeopleSoft Integration Broker to known, necessary endpoints only (NIST AC-4).
4. Step 4: Recovery. Before restoring internet-facing access, validate that network controls are in place, credential rotation is complete, and no unauthorized accounts or scheduled tasks remain. Enable enhanced audit logging on all PeopleSoft application and database tiers (NIST AU-2, AU-12, CIS 8.2). Confirm integrity of HR, payroll, finance, and student record datasets against known-good backups. Monitor for reinfection indicators, including re-appearance of blocked IOCs and new outbound file transfer activity.
5. Step 5: Post-Incident. Assess whether your organization's PeopleSoft deployment follows least-privilege access principles (NIST AC-6, CIS 5.4). Review whether multi-factor authentication (MFA) is enforced on all PeopleSoft administrative and remote access paths (NIST IA-2, CIS 6.3, 6.4, 6.5). Evaluate whether hardcoded or default credentials exist in integration configurations (CIS 4.7, NIST IA-5). Document gaps and schedule remediation as part of your vulnerability management process (CIS 7.1, 7.2). Confirm your incident response plan covers ERP-specific data breach notification obligations given the categories of data at risk.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to legal counsel and executive leadership if forensic analysis of Oracle Unified Audit Trail or PSACCESSLOG confirms bulk SELECT or export operations against HR PERSONAL_DATA, compensation, finance, or student record tables, as this constitutes a probable data breach triggering FERPA, state breach notification statutes, and/or sector-specific regulatory obligations — or if the organization lacks the capability to isolate PeopleSoft from the internet within 4 hours of detection given active ShinyHunters exploitation with no available Oracle patch.
Recovery Notes	Before re-enabling any external PeopleSoft access, require a documented sign-off confirming: (1) all unauthorized accounts removed from PSOPRDEFN, (2) all service account and admin credentials rotated, (3) Integration Broker node allowlist enforced, and (4) enhanced database auditing active on all sensitive data tables. Given ShinyHunters' known pattern of re-targeting previously compromised organizations for secondary extortion, maintain elevated monitoring of PIA authentication logs, outbound proxy logs for connections to new or previously blocked IPs, and PSOPRDEFN for new account creation for a minimum of 30 days post-recovery. Watch the Oracle CPU page and Oracle Security Alerts (https://www.oracle.com/security-alerts/ — validate URL before use) daily until an official advisory or emergency patch is released, and treat patch application as a zero-SLA remediation action the moment one becomes available.
Forensic Artifacts	PeopleSoft PIA WebLogic access log ($PS_CFG_HOME/webserv//servers/PIA/logs/PIA_access.log) — will contain ShinyHunters' credential spray attempts as high-frequency POST requests to /psp/ and /psc/ URI paths, followed by successful 200-response logons from attacker-controlled IPs \| Oracle database Unified Audit Trail (UNIFIED_AUDIT_TRAIL view) or DBA_AUDIT_TRAIL — will record bulk SELECT, export, or EXPDP operations against HR, payroll, finance, and student record tables during the attacker dwell period, establishing the scope of data exfiltrated for breach notification \| PeopleSoft PSACCESSLOG database table — stores application-layer logon/logoff events with OPRID, timestamp, and client IP; cross-correlate with PIA access log to confirm which operator IDs ShinyHunters successfully authenticated as and the duration of their sessions \| Integration Broker gateway log ($PS_CFG_HOME/webserv//servers/PIA/logs/IB_.log) and integrationGateway.properties — will reveal whether the vulnerability chain involved unauthorized inbound service calls to Integration Broker endpoints, and whether attacker-controlled external nodes were registered or called during the attack | File system timeline on PeopleSoft web application directories ($PS_HOME/webserv//applications/peoplesoft/) — mtime/ctime anomalies will identify web shells or backdoor files dropped by ShinyHunters as a persistence mechanism following initial exploitation, corroborated by SHA-256 hash comparison against Oracle-provided PeopleTools installation manifest

Per-Action IR Details

Step 1: Containment — Immediately restrict external access to PeopleSoft web-facing components (PIA, Integration Broker endpoints) at the network perimeter. Apply IP allowlisting or take internet-facing PeopleSoft instances offline if business operations permit. No Oracle patch is available; network isolation is the primary containment control until one is released. Reference: NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers).

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement), 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-hosted PeopleSoft: use iptables to drop all inbound TCP 443/8443 traffic except known business IP ranges — `iptables -I INPUT -p tcp --dport 443 ! -s -j DROP`. On Windows Server: use Windows Firewall with Advanced Security (wf.msc) to create an inbound rule scoping PIA port (default 443) to allowlisted source IPs. For Integration Broker (default port 8443), apply the same rule. Validate with `netstat -an | grep LISTEN` or `ss -tlnp` to confirm no unintended open listeners remain. Two-person verification: one applies rule, second confirms from an external IP that the connection is refused.

Evidence: Before isolating, capture a full netstat snapshot documenting all active connections to PeopleSoft PIA (port 443) and Integration Broker (port 8443) — `ss -tnp` or `netstat -antp` — to preserve active attacker session data. Export current firewall connection state and any NAT/PAT translation tables from the perimeter device. Capture web server access logs (WebLogic access log at `$PS_CFG_HOME/webserv//servers/PIA/logs/access.log`) to preserve ShinyHunters' pre-isolation request patterns before log rotation. Snapshot running processes on the PeopleSoft application server (`ps aux` / `tasklist /v`) to identify any active shells or staging processes spawned prior to cutoff.

Step 2: Detection — Review authentication logs for credential spraying patterns: high-volume failed logons against PeopleSoft PIA login endpoints, followed by successful logon from the same or related source IPs (NIST AU-6, AU-2). Hunt for anomalous shell execution or script invocation from PeopleSoft application server processes. Check for new local or application accounts created outside your provisioning process (CIS 5.1, NIST AC-2). Review file transfer logs and outbound connections for bulk data staging activity. IOCs from exposed attacker infrastructure should be applied to SIEM, firewall, and proxy block lists as they are released by threat intelligence providers — no confirmed public IOC list was available at time of writing.

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-2 (Event Logging), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, run grep-based analysis directly against WebLogic access logs: `grep -E 'POST /psp/.*signonresult|POST /psp/.*signon' access.log | awk '{print $1}' | sort | uniq -c | sort -rn` to surface high-frequency source IPs hitting PIA login endpoints. For shell detection, deploy Sysmon with SwiftOnSecurity config and filter Event ID 1 (Process Create) for parent processes matching `psappsrv.exe`, `PSADMIN.exe`, or WebLogic `java.exe` spawning `cmd.exe`, `powershell.exe`, `sh`, or `bash`. For account enumeration, query PeopleSoft's PSOPRDEFN table via SQL: `SELECT OPRID, OPRDEFNDESC, LASTUPDDTTM FROM PSOPRDEFN WHERE LASTUPDDTTM > SYSDATE - 7 ORDER BY LASTUPDDTTM DESC` to identify recently created operator IDs outside your provisioning window. Monitor outbound TCP connections from the app server using Wireshark or `tcpdump -i eth0 -w capture.pcap 'dst port 443 or dst port 21 or dst port 22'` to catch bulk data exfiltration.

Evidence: Collect PeopleSoft PIA authentication logs from `$PS_CFG_HOME/webserv//servers/PIA/logs/PIA_access.log` and WebLogic server log at `$PS_CFG_HOME/webserv//servers/PIA/logs/PIA_server.log` — these will show credential spray attempts against `/psp/` and `/psc/` URIs. Pull PeopleSoft application server log (`$PS_HOME/appserv//LOGS/APPSRV_MMDD.LOG`) for signs of abnormal integration or query execution. Query the PSACCESSLOG table in the PeopleSoft database for logon/logoff timestamps correlated to suspicious source IPs. Capture PeopleSoft Integration Broker transaction logs for unauthorized inbound/outbound service calls. If Windows-hosted, collect Windows Security Event Log filtering Event ID 4720 (account created), 4728/4732 (group membership changes), and 4624/4625 (logon success/failure) from the PeopleSoft application server host.

Step 3: Eradication — No Oracle patch is available as of this report. Monitor Oracle's Critical Patch Update (CPU) page and security alerts channel for an emergency advisory. In the interim: audit all PeopleSoft accounts and disable or remove accounts not required for operations (CIS 5.3, NIST AC-2); rotate all PeopleSoft service account and administrative credentials immediately (D3-CRO); audit integration configurations for hardcoded credentials (CWE-798 mitigates via D3-CH); restrict PeopleSoft Integration Broker to known, necessary endpoints only (NIST AC-4).

NIST Phase: Eradication

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

Controls: NIST AC-2 (Account Management), NIST AC-4 (Information Flow Enforcement), NIST AC-6 (Least Privilege), CIS 5.3 (Disable Dormant Accounts), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: To audit PeopleSoft operator accounts without enterprise IAM tooling, query: `SELECT OPRID, OPRDEFNDESC, ACCTLOCK, LASTUPDDTTM FROM PSOPRDEFN ORDER BY LASTUPDDTTM DESC` — disable any account with ACCTLOCK=0 that does not appear in your authorized user register. For Integration Broker hardcoded credential audit, grep the PeopleSoft configuration directory: `grep -rn 'password\|passwd\|pwd' $PS_HOME/appserv//psappsrv.cfg` and review node network configuration in the IB Gateway (`$PS_CFG_HOME/webserv//applications/peoplesoft/PSIGW.war/WEB-INF/integrationGateway.properties`) for cleartext credentials. To restrict Integration Broker endpoints, edit `integrationGateway.properties` to allowlist only known node IP addresses and redeploy. Assign one analyst to credential rotation, one to IB endpoint audit — document all changes with timestamps for post-incident review.

Evidence: Before disabling accounts or rotating credentials, dump the full PSOPRDEFN table snapshot and PSROLEUSER table to preserve ShinyHunters' account creation forensics — `SELECT * FROM PSOPRDEFN` and `SELECT * FROM PSROLEUSER WHERE LASTUPDDTTM > `. Export the Integration Broker gateway log (`$PS_CFG_HOME/webserv//servers/PIA/logs/IB_.log`) to preserve records of unauthorized node-to-node calls that may have been used to traverse the vulnerability chain. Capture file system timestamps (`ls -la --full-time` or `Get-Item` in PowerShell) on PeopleSoft web application directories to identify web shells or dropped files introduced during the compromise. Hash all files in `$PS_HOME/webserv//applications/` using SHA-256 (`find . -type f -exec sha256sum {} \;`) to establish a post-incident baseline and detect re-introduction.

Step 4: Recovery — Before restoring internet-facing access, validate that network controls are in place, credential rotation is complete, and no unauthorized accounts or scheduled tasks remain. Enable enhanced audit logging on all PeopleSoft application and database tiers (NIST AU-2, AU-12, CIS 8.2). Confirm integrity of HR, payroll, finance, and student record datasets against known-good backups. Monitor for reinfection indicators, including re-appearance of blocked IOCs and new outbound file transfer activity.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AC-2 (Account Management), CIS 8.2 (Collect Audit Logs), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Enable PeopleSoft application-level auditing by activating Audit Logging in PeopleTools Security (PeopleTools > Security > Audit Logging) for PSOPRDEFN, PSROLEUSER, and key business data components (HR PERSONAL_DATA, PAYROLL_DATA equivalents). At the database tier, enable Oracle Unified Auditing or standard audit policies: `AUDIT SELECT, INSERT, UPDATE, DELETE ON HR.PERSONAL_DATA BY ACCESS`; forward these to a dedicated syslog server or write to a read-only audit partition. For scheduled task validation on Linux: `crontab -l -u ` and `ls -la /etc/cron.*`; on Windows: `schtasks /query /fo LIST /v | findstr /i 'peoplesoft\|psappsrv\|oracle'`. Validate data integrity by running row-count and checksum comparison against the most recent pre-incident backup snapshot for PERSONAL_DATA, compensation, and finance tables — document delta for legal hold.

Evidence: Before bringing PeopleSoft back online, collect a final forensic image of web application directories and app server configuration as post-eradication baseline. Pull the database audit trail for the full incident window covering SELECT operations on HR, payroll, finance, and student tables — ShinyHunters' exfiltration methodology characteristically involves bulk SELECT queries or direct table exports, which will appear in Oracle audit logs (`DBA_AUDIT_TRAIL` or Unified Audit `UNIFIED_AUDIT_TRAIL`). Verify no new cron jobs or Windows Scheduled Tasks reference PeopleSoft process IDs introduced post-compromise. Confirm outbound proxy or firewall logs show zero connections to previously identified attacker staging IPs before re-enabling external access.

Step 5: Post-Incident — Assess whether your organization's PeopleSoft deployment follows least-privilege access principles (NIST AC-6, CIS 5.4). Review whether MFA is enforced on all PeopleSoft administrative and remote access paths (CIS 6.3, 6.4, 6.5; D3-MFA). Evaluate whether hardcoded or default credentials exist in integration configurations (CIS 4.7). Document gaps and schedule remediation as part of your vulnerability

management process (CIS 7.1, 7.2). Confirm your incident response plan covers ERP-specific data breach notification obligations given the categories of data at risk.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For MFA on PeopleSoft PIA without a commercial SSO platform, implement SAML 2.0 federation using PeopleTools' native Signon PeopleCode with a free IdP such as Keycloak (open source) configured to require TOTP as a second factor — Keycloak supports SAML SP integration with PeopleSoft PIA documented in Oracle's PeopleTools Integration Broker administration guide. For least-privilege review, export PSROLEUSER and cross-reference against a job function matrix: `SELECT A.OPRID, A.ROLENAME, B.OPRDEFNDESC FROM PSROLEUSER A JOIN PSOPRDEFN B ON A.OPRID=B.OPRID ORDER BY A.ROLENAME` — flag any non-admin account holding PeopleSoft roles in the PT_SECURITY or ALLPAGES permission lists. For default credential check: compare all PSOPRDEFN entries against Oracle's documented default PeopleSoft accounts (PS, VP1, PTDMO, PEOPLE) and verify each is either disabled or has had its password changed from factory default.

Evidence: Compile a lessons-learned evidence package including: the full PSOPRDEFN/PSROLEUSER delta between pre-incident baseline and post-recovery state (attacker account artifacts), timeline of attacker dwell from first anomalous PIA authentication to containment (sourced from PSACCESSLOG and web access logs), database audit records showing which specific tables and row counts were accessed or exported during the intrusion window (for breach notification scope determination), and Integration Broker transaction logs confirming whether data was exfiltrated via IB service calls versus direct database queries. Retain all forensic artifacts under legal hold given ShinyHunters' extortion model and the likelihood of regulatory breach notification obligations under FERPA (student records), state privacy statutes, or sector-specific requirements depending on the affected organization type.

Detection Guidance

Focus detection on four areas. First, credential spraying: query authentication logs for more than 5 failed PeopleSoft PIA logon attempts from a single source IP within 10 minutes, followed by a successful logon, consistent with T1110.001 and T1110.003 (NIST AU-6, AU-2). Tune the threshold (5 attempts in 10 minutes) based on your environment baseline and false-positive rate. Second, account creation: alert on any new user or service account created within PeopleSoft outside your standard provisioning workflow, particularly accounts with elevated roles (NIST AC-2, CIS 5.1). Third, code execution: monitor PeopleSoft application server process trees for unexpected child processes, particularly shell interpreters (T1059, T1059.004). Fourth, data staging and exfiltration: alert on large outbound file transfers or unusual connections to external IPs from PeopleSoft application or database servers (T1105, T1071.002). Apply IOCs from attacker infrastructure to SIEM, firewall, and DNS block lists as verified IOC lists become available from CISA, Oracle advisories, and threat intelligence providers. System file integrity monitoring on PeopleSoft configuration and init files is also warranted given the reported attack chain (NIST SI-7).

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://www.bleepingcomputer.com/news/security/oracle-peoplesoft-servers-hacked-in-shinyhunters-data-theft-attacks/`	BleepingComputer reporting on the campaign — primary news source; visit for any published IOCs as the story develops	LOW

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1078.001** — Default Accounts
- **T1059.004** — Unix Shell
- **T1657** — Financial Theft
- **T1110.001** — Password Guessing
- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application
- **T1136** — Create Account
- **T1133** — External Remote Services
- **T1105** — Ingress Tool Transfer
- **T1021.004** — SSH
- **T1059** — Command and Scripting Interpreter
- **T1110.003** — Password Spraying
- **T1071.002** — File Transfer Protocols
- **T1021** — Remote Services

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation

- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **CA-7** — Continuous Monitoring
- **AC-3** — Access Enforcement
- **SI-10** — Information Input Validation
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A03:2021** — Injection
- **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
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **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

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

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

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
T1486	Data Encrypted for Impact	Impact
T1078.001	Default Accounts	Defense-Evasion
T1059.004	Unix Shell	Execution

Technique ID	Technique Name	Tactic
T1657	Financial Theft	Impact
T1110.001	Password Guessing	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access
T1136	Create Account	Persistence
T1133	External Remote Services	Persistence
T1105	Ingress Tool Transfer	Command-And-Control
T1021.004	SSH	Lateral-Movement
T1059	Command and Scripting Interpreter	Execution
T1110.003	Password Spraying	Credential-Access
T1071.002	File Transfer Protocols	Command-And-Control
T1021	Remote Services	Lateral-Movement

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/oracle-peoplesoft-se...	T3
Security Testing of On-Premises Products - Oracle	https://www.oracle.com/corporate/security-practices/testing/on-prem...	T3
Oracle PeopleSoft Security: Architecture, Threats & Patch History...	https://rublon.com/blog/oracle-peoplesoft-security-architecture-thr...	T3
Accelerating Vulnerability Detection and Response at Oracle | security	https://blogs.oracle.com/security/accelerating-vulnerability-detect...	T3
CVE-2025-30747 Detail - NVD	https://nvd.nist.gov/vuln/detail/CVE-2025-30747	T1

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 2026-06-10 19:20 UTC by TJS Security Command Center