WARATEK

Securing Oracle PeopleSoft

The 2026 Guide to PeopleSoft Threats, Best Practices, and Automated Runtime Protection

Waratek | August 2026

Table of Contents

Executive Summary

Oracle PeopleSoft runs the operations that keep large enterprises, universities, and public agencies moving such as human resources, payroll, financials, and student records on a single, deeply customized platform. That concentration of sensitive data is exactly what makes PeopleSoft one of the most attractive ERP targets in the world.

The past year removed any doubt. In June 2026 Oracle issued an out-of-band Security Alert for CVE-2026-35273, a CVSS 9.8 unauthenticated remote-code-execution flaw in PeopleTools. The ShinyHunters extortion group had already been exploiting it as a zero-day. Mandiant observed activity between May 27 and June 9, 2026, roughly two weeks before Oracle's advisory, and claimed compromise of more than 300 instances across over 100 organizations, with universities disproportionately hit. Nissan confirmed a data breach tied to the campaign.

This guide combines Waratek's PeopleSoft security best-practices handbook with practical, up-to-date threat intelligence. It covers:

- The 2025–2026 PeopleSoft threat landscape, including the CVEs currently being exploited in the wild and what a decade of PeopleSoft attacks teaches us about patch-lag risk.
- The vulnerability classes that most commonly affect PeopleSoft including insecure deserialization, SSRF/XXE in the Integration Broker, PS_TOKEN forgery, injection, and default-credential exposure with concrete mitigations.
- Hardening best practices across configuration, authentication, network segmentation, and monitoring, updated for Oracle's new monthly Critical Security Patch Update cadence, plus a consolidated checklist.
- Why perimeter and scanning tools (WAF, SAST, DAST) fall short for PeopleSoft, and how Waratek's runtime platform including RASP for production protection and the newly launched Waratek IAST for pre-production testing closes the gap with near zero false positives, no code changes, and no perceivable performance impact.

The core lesson is the same one EBS customers learned in 2025: attackers now weaponize ERP flaws before, or within days of, a patch.

Patching remains essential, but it is no longer sufficient on its own. PeopleSoft owners need protection that works at runtime, inside the application, from day zero.

The 2025–2026 PeopleSoft Threat Landscape

PeopleSoft has always attracted attackers. It is Java-based, internet-reachable in many deployments, built on a middleware stack (WebLogic, Tuxedo) with its own history of critical bugs, and directly connected to payroll, financial, and personnel data. The 2026 ShinyHunters campaign is the most severe example, but it sits at the end of a decade-long pattern.

CVE-2026-35273: The ShinyHunters Zero-Day (CVSS 9.8)

On June 10, 2026, Oracle published an out-of-band Security Alert for CVE-2026-35273, an unauthenticated remote code execution flaw in the Updates Environment Management component of PeopleSoft Enterprise PeopleTools, affecting versions 8.61 and 8.62. No credentials, no user interaction, and low attack complexity: an attacker with HTTP access could execute arbitrary code over the network.

The timeline is the alarming part. Mandiant reported active exploitation in the wild between May 27 and June 9, 2026 as a zero-day, roughly two weeks before Oracle's advisory existed. ShinyHunters reportedly chained older bugs with the zero-day into a "gadget chain," and demonstrated deep familiarity with PeopleSoft internals: extracting credentials from psappsrv.cfg application-server configuration files, mapping connected nodes, and identifying web, application, and batch tiers.

The group claimed compromises of more than 300 instances across over 100 organizations, with roughly 68% of notified organizations in higher education. Ransom notes titled README-IF-YOU-SEE-THIS-YOUVE-BEEN-HACKED.TXT appeared on victim systems, and staging infrastructure held MeshCentral remote-access agents, credential-spray scripts, and defacement tooling purpose-built for PeopleSoft. Nissan later confirmed a breach of data tied to the campaign.

PS_TOKEN Forgery — the "TokenChpoken" Class (Recurring)

PeopleSoft's single sign-on relies on a signed cookie, PS_TOKEN, whose signature is essentially a SHA-1 hash of known fields plus a shared "Node password." Default node names are predictable (PSFT_HR, PSFT_FIN), so an attacker who captures a token knows every input except the node password.

If that password is weak, it can be brute-forced offline and a forged token for the default PS superuser grants full application access without ever knowing a real credential.

When first demonstrated, an estimated 42% of internet-exposed PeopleSoft systems were vulnerable and roughly 10% still used the default node password. Vulnerability scanners still flag “SSO weak secret key” today. Because trusted instances share the node secret, a breach of one low-sensitivity system (say, a test Campus Solutions instance) can pivot into HR or Financials production, the essence of “token chaining.”

Integration Broker SSRF / XXE (Recurring)

The PeopleSoft Integration Broker (IB) processes inbound XML at endpoints such as /PSIGW/PeopleSoftServiceListeningConnector. Crafted XML has repeatedly enabled XML External Entity (XXE) and server-side request forgery attacks that read local files, notably integrationGateway.properties, which holds IB credentials encrypted with a default 3DES key or force the server to reach internal systems. A classic chain turns an unauthenticated file read into full application-server compromise by overwriting gateway configuration to load malicious Java classes.

Inherited Middleware Flaws: WebLogic and Tuxedo/Jolt

Because PeopleSoft runs on WebLogic and Oracle Tuxedo, it inherits their vulnerabilities. CVE-2017-10271 (WebLogic deserialization RCE) was mass-exploited to install cryptominers on PeopleSoft servers.

One campaign enslaved over 700 servers and netted more than $200,000 in Monero. The 2017 “JoltandBleed” set of Tuxedo Jolt vulnerabilities (including CVE-2017-10269) allowed memory disclosure and complete PeopleSoft compromise where the Jolt port was reachable. The lesson: an unpatched middleware layer is a PeopleSoft exposure even when PeopleSoft code is clean.

Recent and Notable PeopleSoft CVEs at a Glance

CVE	Component	CVSS	Impact	Status
CVE-2026-35273	PeopleTools — Updates Environment Management	9.8	Unauthenticated remote code execution	Exploited as zero-day by ShinyHunters from May 2026; out-of-band patch Jun 2026
CVE-2025-30697	PeopleTools — Panel Processor	~6.5	Low-priv unauthorized read/write to backend data via HTTP	Patched 2025
CVE-2025-30747	PeopleSoft CRM	~7.2	Session fixation; session hijacking	Patched 2025
CVE-2020-14592	PeopleTools Rich Text Editor	~6.1	Unauthenticated XSS; session-token theft	Patched; historical
CVE-2018-2919	Unified Navigation (Portal)	~5.4	Cross-instance access-control bypass	Patched; historical
CVE-2017-10271	WebLogic (PeopleSoft stack)	7.5	Deserialization RCE; cryptomining at scale	Still exploited on unpatched systems
CVE-2017-10269	Tuxedo Jolt (“JoltandBleed”)	9.9	Memory disclosure; full PeopleSoft compromise	Patched; historical

Three lessons stand out.

First, attackers exploit PeopleSoft flaws before patches exist (CVE-2026-35273) or reuse timeless techniques (token forgery, SSRF, default credentials) that never fully go away.

Second, the whole stack is in scope: PeopleTools, the Integration Broker, WebLogic, and Tuxedo are all attack surface.

Third, unauthenticated, network-reachable flaws keep recurring, so any PeopleSoft instance with internet-facing components must assume it is being scanned today.

Apply Oracle's Critical Patch Updates, monthly Critical Security Patch Updates, and out-of-cycle Security Alerts immediately and pair them with runtime protection for the window when no patch exists for zero-day protection and defense in depth.

Understanding PeopleSoft and Why It's Hard to Secure

PeopleSoft follows a classic three-tier design known as the PeopleSoft Internet Architecture (PIA). Understanding the tiers is essential to understanding where attacks land.

Tier	What It Does (and Why Attackers Care)
Web Server Tier	Browser-facing front end built on JSP/servlets, typically hosted on Oracle WebLogic. Renders the UI and hosts integration endpoints. Internet-reachable, the primary external attack surface, including the WebLogic admin console and Integration Broker servlets.
Application Server Tier	Business logic on Oracle Tuxedo, running PeopleCode and enforcing authentication and role-based authorization (the PSAPPSRV processes). Communicates with the web tier over the Jolt protocol. Compromise here means control of security enforcement itself.
Database Tier	All transactional data plus PeopleTools metadata and configuration. The app server connects using a high-privilege Access ID; a low-privilege Connect ID

Tier	What It Does (and Why Attackers Care)
	bootstraps that connection. Holds the crown jewels; payroll, financials, PII, student records.
Integration Broker & Process Scheduler	IB exposes web services for system-to-system integration; the Process Scheduler runs batch jobs. Both interact across tiers and have historically been rich sources of SSRF/XXE and privilege-escalation bugs.

The same qualities that make PeopleSoft valuable make it difficult to secure. Extensive customization and PeopleCode create an enormous, organization-specific attack surface; shared SSO trust between instances means one weak node can cascade; and the layered middleware stack means a flaw in WebLogic or Tuxedo is a PeopleSoft flaw. Deployments are often long-lived, and older versions may still carry static default keys, demo accounts (VP1, PS), and unchanged Connect IDs. Security and convenience will always be in tension; the goal of this guide is to keep the convenience while closing the gaps.

Common Vulnerability Classes in PeopleSoft

Insecure Deserialization

Java applications serialize objects to move data between components, and PeopleSoft through PeopleTools, WebLogic, and Tuxedo exchanges serialized data constantly. Malicious payloads hidden in a byte stream execute when deserialized, enabling remote code execution, authentication bypass, or privilege escalation. CVE-2017-10271 in WebLogic is a deserialization flaw. Mitigate by validating input before deserialization, restricting deserialization to allow-listed classes (Oracle's JEP 290 blocklist filter helps), using safe libraries, and disabling unsafe object-creation hooks.

SSRF and XML External Entity (XXE) Injection

The Integration Broker and PeopleSoft's XML parsers have repeatedly allowed crafted XML to trigger server-side request forgery and external-entity attacks reading local configuration files (including credential-bearing

integrationGateway.properties), forcing outbound requests to internal systems, or, via gopher:// and UNC-path tricks, harvesting SMB hashes. Mitigate by disabling external-entity resolution in XML parsers, validating and allow-listing IB message sources, restricting the gateway's network egress, and replacing default gateway credentials and encryption keys.

PS_TOKEN / SSO Token Forgery

Because PS_TOKEN is signed with a shared node password over predictable node names, a weak secret lets an attacker forge a valid token for any user (including the PS superuser) with no credentials. Mitigate with long, random node passwords; certificate-based node authentication instead of shared passwords; changing default node names; enabling the PeopleTools 8.56+ check-token / callback safeguard (which keeps issued tokens in memory and clears them on restart); and, ideally, disabling native PeopleSoft SSO in favor of a third-party IdP over SAML or OIDC.

Injection (SQL and Command)

Unvalidated input reaching SQL or the operating system lets attackers read or alter data or execute commands. PeopleSoft has patched injection and input-validation flaws across PeopleTools and portal components (for example CVE-2022-21345), and real-world SQL-injection breaches of university PeopleSoft systems have exposed HR and student data. Mitigate with parameterized queries and prepared statements throughout PeopleCode and custom SQL, strict input validation and sanitization, and least-privilege database accounts.

Insufficient Authentication and Authorization

Weak authentication gives attackers an easy window to gain access and escalate privileges. The essentials:

- **Strong password policy:** Enforce complexity, rotation, and no reuse; change every default and demo-account password (VP1, PS, Connect ID, WebLogic console, IB admin).
- **Multi-factor authentication:** Require a second factor (authenticator app, hardware token, or passkeys) for all users, and especially for privileged and administrative access.

- **Session management:** Use session timeouts, automatic logout for inactive sessions, and session-activity monitoring; enable the check-token safeguard to prevent token-based hijacking.
- **Role-based access control:** Configure roles and permission lists for least privilege; scrutinize the “public” / guest user so password-reset and job-listing pages cannot reach internal components.
- **Segregation of duties:** Split critical financial and HR tasks so no single account can both create and approve.
- **Continuous auditing:** Audit access logs and permissions continuously, with automated alerts for anomalies such as off-hours privileged logins.

Default Credentials, Keys, and Secrets

PeopleSoft’s recurring weakness is the secret left at its delivered value. The Connect ID has historically shipped as people/peop1e; the WebLogic console as system/Passw0rd; the Integration Broker gateway as administrator/password; and, before PeopleTools 8.53, config encryption used a single static key shared across all installations. Any one of these can hand an attacker DBA-level control or a deployable webshell. Change every delivered password to a strong, unique value, regenerate cryptographic keys with pskeymanager / pscipher, remove demo accounts, and encrypt configuration files.

Information Exposure and Cleartext Transmission

Sensitive data leaks through verbose error messages, misconfigured report repositories and permissions, and unencrypted transmission. Report URLs that are guessable, or a public user with too many privileges, can expose records to unauthenticated users. Use generic user-facing error messages with detail logged only for authorized staff; enforce strict access on the Report Repository; and encrypt data at rest (AES-256) and in transit. Enforce TLS 1.2+ (PeopleTools 8.60+ supports TLS 1.3) across all PeopleSoft traffic (web tier, Jolt, and database) disable SSL 2.0/3.0 and TLS 1.0/1.1, and restrict to strong cipher suites.

Hardening and Operating Your PeopleSoft Environment

Securing PeopleSoft is not just about responding to threats. It is about actively minimizing your attack surface.

The recent CVEs make one practice non-negotiable:

Patch Management: Oracle's New Monthly Cadence

In 2026 Oracle moved to a monthly security patching rhythm. The familiar quarterly, cumulative Critical Patch Updates (CPUs) released the third Tuesday of January, April, July, and October, and routinely carrying a handful of PeopleSoft fixes are now complemented by monthly Critical Security Patch Updates (CSPUs): smaller, targeted collections of high-priority fixes released on the third Tuesday of the remaining eight months. Oracle publishes a pre-release announcement the Thursday before each release. Out-of-band Security Alerts, like the one for CVE-2026-35273, still ship whenever a flaw is too critical to wait.

- **Treat CSPUs and Alerts with maximum urgency:** CVE-2026-35273 was exploited as a zero-day before its alert existed. Do not defer PeopleSoft fixes to a quarterly cycle.
- **Patch the whole stack:** Apply PeopleTools patches and the underlying WebLogic, Tuxedo, and database CPUs. The 2018 cryptomining wave hit PeopleSoft through an unpatched WebLogic, not PeopleSoft code.
- **Plan for twelve patch events a year:** Replace quarterly windows with a standing monthly window aligned to Oracle's third-Tuesday schedule, using each Thursday pre-release to scope work.
- **Stay informed:** Subscribe to Oracle Security Alert notifications and monitor CISA's Known Exploited Vulnerabilities catalog for PeopleSoft and WebLogic entries.
- **Reduce exposure:** Inventory internet-facing endpoints (/PSIGW/, /console, the PIA sign-in) and remove any not strictly required.

Network Segmentation and Access Control

- Expose only the PIA web tier to users. Keep all app-server, database, Jolt, and Integration Broker traffic internal; the JoltandBleed and integration-gateway attacks depend on reachable internal ports.

- Firewall the Tuxedo Jolt ports (typically 9000/9001), IB ports, and the WebLogic admin console away from untrusted networks; bind the console to localhost or a management network.
- Place PeopleSoft behind a VPN or an authenticating reverse proxy, and restrict access to trusted networks where operations allow.
- Implement HTTP security headers (HSTS, Content-Security-Policy, X-Content-Type-Options, X-Frame-Options) and deploy TLS from trusted CAs, auditing cryptographic settings regularly.

Secure Configuration

- Change all delivered passwords and regenerate default cryptographic keys; encrypt configuration files rather than relying on the static default key.
- Remove demo and sample accounts (VP1, PS, and similar), and review all accounts and node trusts to eliminate unnecessary ones.
- Disable or lock down features you do not use. If the Integration Broker or a given node is not needed, turn it off or firewall it and change its credentials.
- Enable PeopleSoft account lockout and password-complexity controls, and integrate logins with MFA.

Monitoring and Incident Response

- Enable comprehensive logging (PIA/web, application-server, Integration Broker, and database) and centralize it with a SIEM such as Splunk or ELK; set retention to meet regulatory requirements.
- Alert on key indicators of compromise; unexpected Integration Broker calls, high volumes of failed logins (possible token brute-forcing), off-hours privileged access, unusual configuration changes, and unexplained CPU spikes (a cryptomining tell).
- Maintain a written, tested incident response plan with roles, communication protocols, and escalation paths; organizations in the ShinyHunters campaign that had rehearsed plans contained damage faster.

Why Traditional Security Tools Fall Short for PeopleSoft

The manual practices above are essential, but they are time-consuming, complex, and prone to human error. The tools most organizations reach for to automate them each carry heavy drawbacks in a PeopleSoft context.

Web Application Firewalls (WAFs)

WAFs build a solid perimeter and stop plenty of commodity attacks, but they rely on tuned rules for known threats. They struggle with the unique customizations, custom exploit payloads and custom PeopleCode of PeopleSoft applications, generate high false-positive rates that block legitimate traffic, and offer no help against zero-days. A WAF rule for CVE-2026-35273 could not exist during the weeks ShinyHunters was exploiting it. Once an attacker is past the wall (or already inside via a forged token or exposed internal port), the WAF is blind.

SAST and DAST Scanners

Static analysis scans code that never executes, producing high false-positive rates and vulnerability fatigue and it struggles with PeopleCode and heavily customized PeopleSoft extensions where source may not even be available.

Dynamic analysis crawls the application from outside as a black box, missing deep logic flaws and providing no code-level context for fixes. Operating both means extra licenses and testing time, and neither can distinguish a real, exploitable issue from noise. When scanners cry wolf too often, real alerts lose urgency; when they miss, attackers get free reign.

The Waratek Platform: Runtime Security for Oracle PeopleSoft

Waratek takes a fundamentally different approach: security enforced from inside the Java runtime itself, where the application's actual behavior, not signatures or source-code guesses, determines what is malicious. Because PeopleSoft, WebLogic, and Tuxedo are all Java, Waratek protects the whole stack.

For PeopleSoft customers the platform delivers two complementary capabilities: RASP for protecting production, and the newly launched Waratek IAST for finding vulnerabilities before production. Together they form a continuous "Detect-to-Protect" loop from development through production.

Waratek RASP: Protection in Production

Waratek's Runtime Application Self-Protection embeds security policies directly into your PeopleSoft applications' runtime environments. Deployment is as simple as installing Waratek agents across the Java components (WebLogic web tier, PeopleSoft app-server processes, and integration services) with no code changes and no downtime. Key properties:

- **Near zero false positives:** Because Waratek observes actual code execution rather than matching patterns, it distinguishes real attacks from legitimate traffic with almost 100% accuracy. No detective work for your team and no broken PeopleSoft functionality.
- **Real-time protection, known and unknown:** Instantly blocks SQL injection, XSS, CSRF, insecure deserialization, command injection, and related classes at runtime including exploitation of unknown (zero-day) vulnerabilities, closing the patch-lag window that ShinyHunters exploited.
- **Safe deserialization:** For deserialization attacks, the class behind the PeopleTools and WebLogic RCEs, the platform deserializes bytecode in an isolated environment first. Then Waratek studies the effects and sanitizes or blocks malicious payloads before they reach your application.
- **SSRF and injection defense:** Context-aware policies restrict what application code can reach and return, blocking Integration Broker SSRF/XXE and neutralizing SQL injection at runtime regardless of database vendor.
- **Virtual patching in minutes:** Known PeopleSoft and middleware CVEs can be remediated at runtime without application downtime or source changes, cutting patching timelines from weeks to minutes while you schedule the official CPU.

- **No performance penalty:** Waratek runs directly inside the JVM with no perceivable performance hit, and scales simply: spin up a new application and deploy an agent alongside it.
- **Audit-ready reporting:** Every security event is logged with CEF output for your SIEM and for reports to executives and compliance auditors, supporting SOC 2, GDPR, and CCPA obligations.

Waratek IAST: Finding What Scanners Miss

Launched at JavaOne 2026, Waratek IAST (Interactive Application Security Testing) works from within the running application during functional testing to identify real, exploitable vulnerabilities as code actually executes. That's the visibility SAST and DAST fundamentally lack.

- **Perfect OWASP Benchmark score:** 100% true positive rate, 0% false positive rate, and the maximum OWASP Benchmark score of 100 achieved with zero manual tuning or custom rulesets.
- **No source code required:** IAST analyzes compiled bytecode, so it works on PeopleCode-driven customizations and extensions without source access and is indifferent to whether a human or an AI wrote the code.
- **Zero scan time, zero friction:** Runs inside existing CI/CD pipelines with continuous feedback during functional testing. No separate scan windows, no context switching for developers.
- **Instant, actionable findings:** Every finding arrives with full stack traceability and remediation guidance, so teams fix the vulnerable code path, not a symptom. Waratek reports this eliminates 30–40% of manual testing hours.
- **A safety net for AI-generated code:** As teams use AI to accelerate development, including custom PeopleSoft extensions, IAST validates AI-generated code and patterns in your actual runtime, catching the subtle flaws and insecure defaults AI-generated code often introduces.

Paired with RASP, IAST closes the loop: vulnerabilities discovered during testing inform runtime protection policies, and attacks blocked in production inform what to test next.

How Waratek Maps to the Recent CVEs

Threat pattern (recent example)	Waratek coverage
Zero-day RCE via crafted requests (CVE-2026-35273)	Runtime behavioral protection blocks exploit primitives (command execution, malicious deserialization, illegitimate process forking) even when the CVE is unknown and unpatched.
Insecure deserialization (CVE-2025-30748, CVE-2017-10271 WebLogic)	Payloads are deserialized in isolation and sanitized or blocked before reaching the application, neutralizing the class outright with zero false positives.
Integration Broker SSRF / XXE and file disclosure	Context-aware policies restrict what code can reach and return; anomalous outbound requests and local-file access are detected and blocked at runtime.
PS_TOKEN forgery and injection breaches	Granular rules on specific URIs and behaviors block unsafe payloads and anomalous privileged actions, while CEF logs feed your SIEM.

PeopleSoft Security Checklist

Area	Action	Done
Patching	Current on latest quarterly CPU, all monthly Critical Security Patch Updates, and all Security Alerts (incl. CVE-2026-35273 fix)	☐
Patching	Underlying WebLogic, Tuxedo, and database CPUs applied alongside PeopleTools	☐
Patching	Monthly patch window scheduled for Oracle's third-Tuesday cadence; subscribed to Alerts and monitoring CISA KEV	☐

Area	Action	Done
Exposure	Internet-facing endpoints (/PSIGW/, /console, PIA) inventoried and minimized	☐
Credentials	Connect ID, Access ID, WebLogic console, IB gateway, and node passwords changed from defaults; demo accounts (VP1, PS) removed	☐
Crypto keys	Default config-encryption keys regenerated via pskeymanager / pscipher	☐
SSO / Tokens	Long random node passwords or certificate-based node auth; check-token safeguard enabled; native SSO replaced with IdP where possible	☐
Authentication	Strong password policy enforced; MFA enabled for all users and privileged access	☐
Authorization	Least-privilege roles and permission lists; public/guest user scoped; SoD in place; permissions audited	☐
Network	Only PIA web tier exposed; Jolt/IB/console ports firewalled internally; TLS 1.2+ everywhere; strong ciphers only	☐
Integration Broker	External-entity resolution disabled; message sources allow-listed; gateway egress restricted	☐
Monitoring	Centralized logging with SIEM; IoC-based alerting tuned; logs reviewed routinely	☐
Response	Incident response plan documented, communicated, and tested	☐
Runtime protection	RASP agents deployed across PeopleSoft/WebLogic components for zero-day coverage and virtual patching	☐
Testing	IAST integrated in CI/CD for custom PeopleCode and extensions	☐

Get Started with Waratek

Securing Oracle PeopleSoft manually is challenging and resource-intensive — and the 2026 ShinyHunters campaign shows the cost of gaps. Waratek automates your best practices, protects the patch-lag window across PeopleSoft and its middleware, and now tests your code with the same runtime precision it uses to protect it. Deployment is straightforward, integration requires no code changes, and protection begins immediately.

- Request a demo or speak with a security expert.
- Learn more: waratek.com — IAST, RASP, and IAST+RASP solution pages

"An excellent security solution, very easy to implement, and instant protection for vulnerabilities. Waratek's fantastic team supported us through the entire process." — Verified User in Financial Services, G2