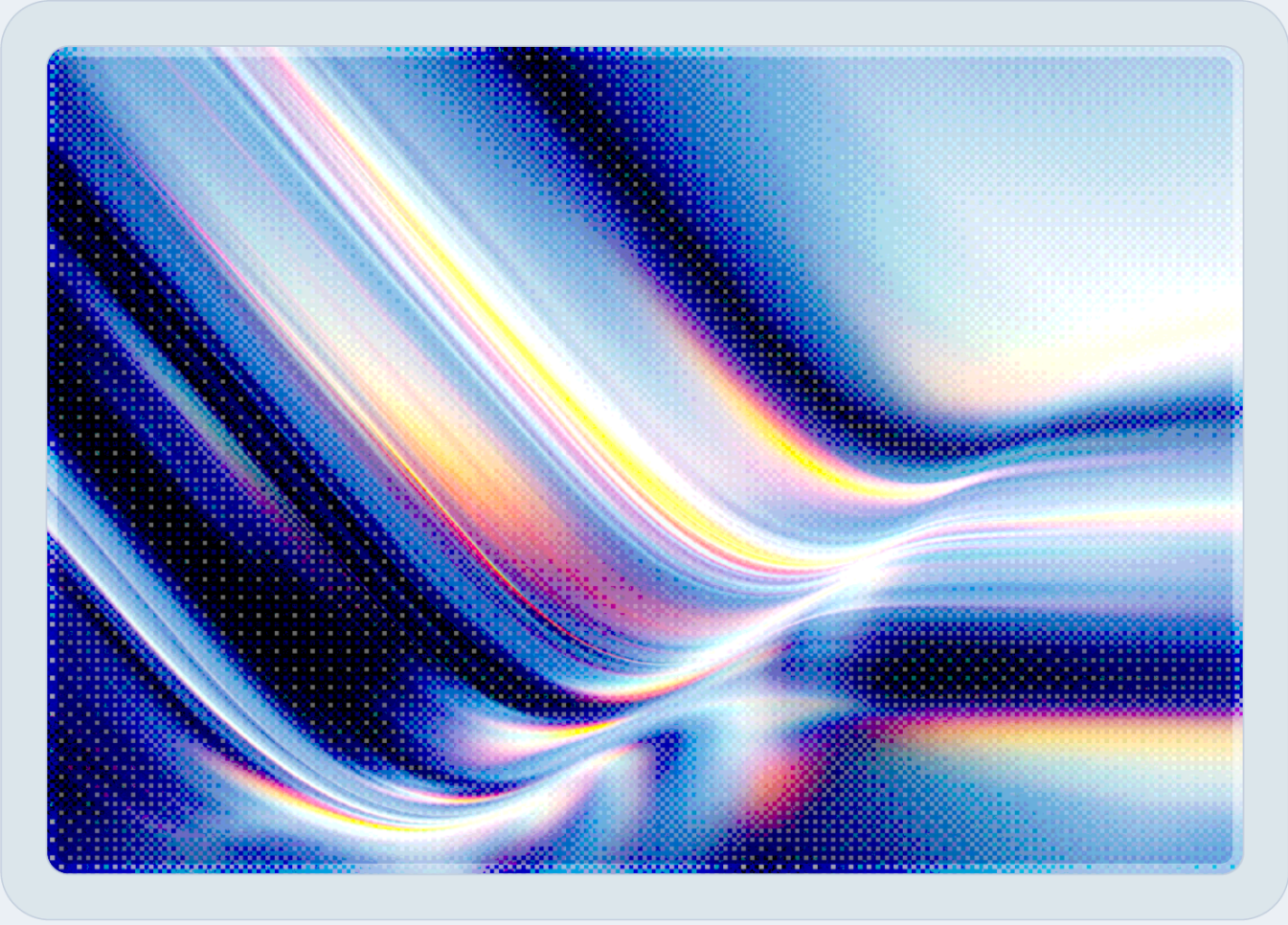
CSAI Foundation | Cloud Security Alliance

Oracle PeopleSoft Zero-Day: ShinyHunters Breaches 100 Universities

CVE-2026-35273 and the Systemic Risk of Shared ERP Infrastructure

2026-06-30

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

Between May 27 and June 9, 2026, the financially motivated threat group ShinyHunters — tracked by Mandiant and the Google Threat Intelligence Group as UNC6240 — exploited a critical zero-day vulnerability in Oracle PeopleSoft's Environment Management component to compromise more than 300 application instances across 100+ organizations [1][2]. The flaw, CVE-2026-35273, carries a CVSS 3.1 score of 9.8 and requires no authentication, no user interaction, and no special access to execute arbitrary code over a standard HTTP connection [3]. Oracle published an out-of-band security advisory and emergency patch on June 10, 2026 — two full weeks after initial exploitation was first observed [4].

Sixty-eight percent of victim organizations operate in the higher education sector, where PeopleSoft is a widely deployed ERP platform for student information, financial aid, human resources, and payroll [2]. The University of Nottingham was among the first confirmed victims, with approximately 454,600 current and former student records exposed — including passport numbers, addresses, and sensitive demographic details such as ethnicity and disability status [5]. The incident is a concrete example of how a single unauthenticated vulnerability in widely shared infrastructure can cascade rapidly across an entire sector before any public disclosure or mitigation guidance exists.

Organizations running PeopleSoft PeopleTools versions 8.61 or 8.62 should apply Oracle's emergency patch immediately and implement the network-level mitigations described in this note.

Background

Oracle PeopleSoft and the Higher Education Market

Oracle PeopleSoft is an enterprise application suite that has served large organizations — particularly public universities and government agencies — for more than three decades. Oracle PeopleSoft has long served as one of the primary ERP platforms in North American higher education, with Campus Solutions deployments particularly concentrated among large public universities. PeopleSoft Campus Solutions manages student records, financial aid disbursements, tuition billing, enrollment workflows, and alumni data. The breadth of personally identifiable information concentrated within these systems — Social Security numbers, immigration status, academic transcripts, healthcare records through campus clinics, and detailed financial profiles — makes them high-value targets for data theft and extortion.

The Environment Management (EM) component at the center of this incident is a PeopleSoft administrative subsystem used to monitor and coordinate multi-server deployments. It runs as a separate hub service (EMHub) and is accessible via the PSIGW integration gateway. In many enterprise deployments, this component is reachable over standard HTTP on the same network-accessible interface used for the PeopleSoft Internet Architecture (PIA) portal, a configuration that substantially expands the attack surface, as it places administrative services on the same network-accessible interface as the end-user portal.

ShinyHunters and Their Operational Model

ShinyHunters (UNC6240) is a financially motivated criminal group active since at least 2020, with documented breaches of more than 400 organizations spanning retail, technology, aviation, finance, and higher education [6]. The group's name derives from the Pokémon concept of shiny hunting — obsessively seeking rare targets — and their operational model is consistent: breach an organization, exfiltrate high-value data, approach the victim privately with a ransom demand, and publish stolen data on dark web forums if payment is refused. The group took over administration of BreachForums, a prominent data-trading marketplace, following the arrest of its original founder in 2023, and maintained that role until the FBI seized the domain in October 2025 [6].

Mandiant and GTIG attribute this campaign to UNC6240 based on infrastructure patterns, tooling signatures, and data posting behavior on ShinyHunters' extortion site [1][2]. As of June 10, 2026, the group claims to have stolen data from organizations comprising 300 compromised PeopleSoft instances, though the number of independently verified victims continues to grow as institutions complete their initial forensic assessments [2][8].

Security Analysis

The Vulnerability: CVE-2026-35273

CVE-2026-35273 is a critical unauthenticated server-side request forgery (SSRF) to remote code execution (RCE) vulnerability in PeopleSoft Enterprise PeopleTools, affecting versions 8.61 and 8.62 [3] [9]. The flaw is catalogued under CWE-306 (Missing Authentication for Critical Function), meaning that a servlet handling sensitive administrative operations can be reached by any HTTP client without presenting valid credentials.

The attack chain proceeds in two stages. First, the attacker sends a crafted HTTP request to the PSIGW integration gateway, exploiting an SSRF condition that allows the gateway to forward the request to an internal administrative servlet that would otherwise be inaccessible from external networks. Second, the forwarded request triggers a Java XMLDecoder deserialization routine within the underlying WebLogic JVM — a class of vulnerability with an extensively documented exploitation history in enterprise Java applications — allowing the attacker to supply a malicious serialized payload that executes arbitrary code with the privileges of the PeopleSoft application server process [9]. The complete attack requires only network access over HTTP, involves no user interaction, and succeeds with low attack complexity, producing the maximum severity CVSS vector of (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) [3].

Oracle's June 10, 2026 advisory confirmed that active exploitation preceded the advisory by approximately two weeks, making this a true zero-day campaign during the exposure window [4]. The vendor rolled a fix into an out-of-band patch, available through My Oracle Support as Patch CPU187, and subsequently included it in the June 2026 Critical Patch Update [4].

Attack Execution: Infrastructure and Lateral Movement

Mandiant and GTIG's investigation documented precise timestamps for attacker staging activity. On May 27, 2026 at 22:14 UTC, ShinyHunters configured a MeshCentral remote management server (version 1.1.59) to serve as their command-and-control infrastructure for the campaign [1][2]. MeshCentral is a legitimate open-source remote management framework; the threat actors configured it to produce Windows binaries with names mimicking Microsoft Azure internal services — specifically `meshagent32-azure-ops.exe`, `meshagent64-azure-ops.exe`, and `meshagent64-v2.exe`; Mandiant assesses that these Azure-mimicking names were chosen to blend with expected cloud infrastructure traffic in monitoring tools [1].

After exploiting CVE-2026-35273 to gain initial code execution on a target PeopleSoft server, the attackers deployed these MeshCentral agents, establishing persistent remote access. From this foothold, they ran administrative command queries against the PeopleSoft database tier to identify and exfiltrate sensitive records. For lateral movement, the attackers used a custom shell script named `[victim_abbreviation]_fanout.sh` — with the prefix customized per-target — that automated SSH credential spraying across internal hosts identified by parsing the server's `/etc/hosts` file for institution-specific naming patterns [1][2]. This approach allowed the attackers to pivot from an externally facing PeopleSoft application server to internal administrative systems without requiring additional vulnerability exploitation. A plaintext ransom marker file, `README-IF-YOU-SEE-THIS-YOUVE-BEEN-HACKED.TXT`, was written to compromised systems in what appears to be both a notification mechanism and evidence of access for extortion purposes [1].

Data Exposure and Regulatory Exposure

PeopleSoft Campus Solutions environments contain some of the most sensitive personal data held by any enterprise system. Depending on institutional configuration, these databases routinely hold student biographical records including legal names, addresses, and contact information; financial data covering tuition payments, financial aid awards, and bank account details for direct deposit; government-issued identification numbers and passport scans required for international enrollment and I-20 visa processing; health records from campus clinics integrated with PeopleSoft's human resources module; human resources files including salary, performance history, and benefit enrollment for faculty and staff; and administrative credentials for the underlying Oracle database and operating system accounts, harvested during the lateral movement phase [7][8].

The University of Nottingham confirmed that approximately 454,600 records were exposed, with the leaked dataset containing names, addresses, telephone numbers, passport numbers, and details on student ethnicity and disability status — categories that attract heightened regulatory scrutiny under GDPR [5]. For US institutions, the exposed student records trigger FERPA notification obligations, and any health data flowing through PeopleSoft's HR or campus clinic integration may require HIPAA breach notifications as well. The 68% concentration of victims in higher education means the regulatory exposure across affected institutions spans at least three major frameworks — GDPR, FERPA, and state breach notification laws — affecting more than 100 organizations, with divergent international notification timelines adding complexity for institutions with campuses or students in multiple jurisdictions [7].

The Shared Infrastructure Amplification Effect

The scale of this incident — 300 compromised instances from a single unauthenticated vulnerability — reflects the structural risk inherent in how enterprise ERP systems are typically deployed in higher education. Many universities contract with managed service providers or Oracle's PeopleSoft Cloud Manager to host their PeopleSoft environments in consolidated or multi-tenant arrangements. In these configurations, a single hosting cluster may serve multiple institutions, and the network trust relationships, SSH key sharing, and internal routing tables that facilitate administration across those environments can be traversed by the fanout.sh lateral movement technique documented in this campaign [2][8]. Even institutions whose PeopleSoft deployments are directly Internet-facing but isolated faced rapid compromise because the initial access required no credential material whatsoever — only HTTP reachability to the PSIGW endpoint.

The incident follows a pattern seen in previous high-impact ERP campaigns, including the exploitation of SAP systems via CVE-2020-6287 (RECON), where a single pre-authentication flaw against a widely deployed enterprise platform produced a large victim count before patch adoption could catch up with

attacker speed [10]. The higher education sector may face particular exposure to this dynamic, given widely documented challenges with decentralized IT governance and the operational constraints that often delay ERP patching during enrollment and financial aid cycles; application-layer monitoring of PeopleSoft endpoints is also less consistently present in institutional SOC tooling than in more mature enterprise environments.

Recommendations

Immediate Actions

Organizations running PeopleSoft PeopleTools versions 8.61 or 8.62 should treat this as an emergency patching event. Oracle's out-of-band patch (CPU187) is available through My Oracle Support and should be applied as soon as change management processes allow — ideally within 24 to 72 hours given confirmed active exploitation. While the patch is being staged, network-level mitigations can substantially reduce risk. PeopleSoft administrators should disable the Environment Management Hub (EMHub) Service in multi-server configurations, or remove the PSEMHUB application entirely in single-server deployments [4][9]. Environments where EMHub cannot be immediately disabled should block all external access to the URL paths `/PSEMHUB/*` and `/PSIGW/HttpListeningConnector` at the network perimeter or application firewall layer; Mandiant assesses that restricting these endpoints does not impair normal end-user PeopleSoft Internet Architecture (PIA) browser sessions [1].

Organizations should also immediately audit outbound network connections from their PeopleSoft application servers. The MeshCentral-based C2 infrastructure used in this campaign generates outbound HTTPS traffic to cloud-hosted endpoints, and unusual outbound SMB traffic (TCP port 445) from application servers to external destinations indicates potential credential relay or pivoting activity [1][9]. Threat hunting queries for the MeshCentral agent binary names documented by Mandiant (`meshagent32-azure-ops.exe`, `meshagent64-azure-ops.exe`) against endpoint detection and endpoint logs should be run across all servers in the PeopleSoft hosting environment.

Short-Term Mitigations

Beyond the immediate patch and network controls, institutions should conduct a full review of administrative credentials and SSH keys on PeopleSoft application servers and any downstream systems reachable from those servers. The fanout.sh lateral movement technique uses credential material harvested from the initial compromise server; any credentials that were present on compromised

systems must be assumed exposed and rotated. This includes database connection strings stored in PeopleSoft configuration files, service account passwords, and any SSH private keys used by administrative automation scripts [2][8].

Institutions that experienced confirmed compromise should engage their incident response procedures promptly and prepare for regulatory notification. Under GDPR, breaches involving personal data must be reported to the relevant supervisory authority within 72 hours of awareness of the breach [7][15]. FERPA does not specify a notification window but requires notification to affected students, and many US states impose their own breach notification timelines. Given the sensitivity categories present in PeopleSoft databases — passport numbers and disability status were confirmed exposed in the Nottingham incident — institutions should assume the highest-sensitivity data categories were accessible during the exploitation window and scope notifications accordingly.

Strategic Considerations

This incident provides a concrete case for accelerating two strategic changes in how higher education institutions manage ERP security. First, patch latency for critical ERP vulnerabilities must be reduced. Enterprise ERP environments — particularly in higher education — have historically operated on extended patch cycles, with operational risk tolerance around enrollment and financial aid periods often further delaying remediation; CVE-2026-35273 was exploited for 14 days before Oracle issued guidance, and institutions that had not applied the fix within days of the June 10 advisory remained exposed through the end of the month. Institutions should establish a tiered patch SLA that treats CVSS 9.0+ vulnerabilities in Internet-reachable ERP components as requiring emergency patching within 72 hours, with a corresponding pre-approved change window for such circumstances.

Second, the attack surface created by exposing EMHub and PSIGW endpoints to the Internet is architecturally unnecessary. PeopleSoft's end-user PIA interface requires external access; its administrative components do not. Institutions should place administrative ERP services behind a zero trust network access (ZTNA) policy that requires verified identity and device posture before any connection to administrative endpoints is permitted, regardless of network location. This architecture would have significantly reduced the attack surface, as the vulnerable endpoint would not have been reachable by unauthenticated external clients — the exploitation vector documented in this campaign — without prior identity and device verification.

Managed service providers and cloud hosting arrangements that serve multiple institutions on shared PeopleSoft infrastructure should conduct an immediate review of network isolation controls, cross-tenant trust relationships, and the credential sharing practices that enable the SSH lateral movement observed in this campaign. The "shared infrastructure" framing in this incident description is meaningful:

when a threat actor can move from a compromised instance at Institution A to systems belonging to Institution B via shared hosting trust relationships, the individual institution's patching discipline alone cannot bound the blast radius.

CSA Resource Alignment

Several established CSA frameworks address the vulnerabilities exploited in this campaign, spanning enterprise resource planning security and cloud-hosted business-critical applications. CSA's **Top 20 Critical Controls for Cloud ERP Customers** identifies vulnerability management (TVM), identity and access management (IAM), and network security as foundational control domains for cloud-hosted ERP environments, and specifically flags unauthenticated API endpoints and insecure integration gateways as high-priority risks [11]. The five control domains in that framework — Cloud ERP Users, Cloud ERP Application, Integrations, Cloud ERP Data, and Business Processes — all have direct bearing on the attack pattern observed here, with the Integration domain control most directly applicable to the vulnerable PSIGW gateway.

The **Cloud Controls Matrix (CCM) v4.1** provides a control mapping vocabulary for assessing and remedying the gaps exploited in this campaign [12]. Relevant control domains include TVM-01 through TVM-09 (Threat and Vulnerability Management), which covers patch management policy, patch SLA definitions, and vulnerability scanning; IAM-01 through IAM-13 (Identity and Access Management), which addresses authentication requirements for all access paths including administrative services; and IVS-06 through IVS-09 (Infrastructure and Virtualization Security), which covers network segmentation and perimeter controls for cloud-hosted systems.

CSA's **STAR program** provides a mechanism for verifying that third-party managed service providers maintaining PeopleSoft environments have adequate security controls in place [13]. Institutions relying on hosted ERP environments should require their vendors to publish a CSA STAR Level 2 attestation or equivalent assurance evidence, with explicit coverage of patch management SLAs for critical vendor-published vulnerabilities and network isolation controls between tenant environments.

The Zero Trust principles articulated in CSA's **Software Defined Perimeter and Zero Trust** guidance are directly applicable to the architectural remediation described in the Recommendations section [14]. Placing administrative ERP services behind a zero trust access policy — requiring cryptographic identity verification and device health attestation before any administrative endpoint is reachable — represents the structural control that would have blocked the initial exploitation vector in this campaign.

References

[1] Mandiant / Google Threat Intelligence Group. "ShinyHunters Targets Education Sector with Oracle PeopleSoft Exploit." Google Cloud Blog, June 2026.

[2] The Register. "ShinyHunters hacked 100+ orgs by exploiting an Oracle PeopleSoft 0-day." The Register, June 11, 2026.

[3] NIST National Vulnerability Database. "CVE-2026-35273 Detail." NVD, June 2026.

[4] Oracle Corporation. "Oracle Security Alert Advisory – CVE-2026-35273." Oracle, June 10, 2026. (Access may require My Oracle Support account; core claims corroborated by [1], [2], [9], [10].)

[5] BleepingComputer. "Nottingham University data breach affects over 450,000 students." BleepingComputer, June 2026.

[6] Security Boulevard. "ShinyHunters: The Group Behind 300+ Breaches." Security Boulevard, May 2026. (Page may be access-restricted; claims corroborated by independent sources.)

[7] Cybersecurity Dive. "ShinyHunters linked to exploitation of critical flaw in Oracle PeopleSoft." Cybersecurity Dive, June 2026.

[8] Black Kite. "ShinyHunters Hit Oracle PeopleSoft and Your Vendors May Already Be Compromised." Black Kite, June 2026.

[9] Rapid7. "Active Exploitation of Oracle PeopleSoft Zero-Day (CVE-2026-35273)." Rapid7, June 2026.

[10] SecurityWeek. "Oracle Addresses PeopleSoft Vulnerability Amid Reports of Zero-Day Attacks." SecurityWeek, June 2026.

[11] Cloud Security Alliance. "Top 20 Critical Controls for Cloud Enterprise Resource Planning (ERP) Customers." CSA, 2019.

[12] Cloud Security Alliance. "Cloud Controls Matrix v4.1." CSA.

[13] Cloud Security Alliance. "CSA STAR Program." CSA.

[14] Cloud Security Alliance. "Software Defined Perimeter and Zero Trust." CSA, 2020.

[15] European Parliament. "Regulation (EU) 2016/679 – Article 33." Official Journal of the European Union, April 2016.