Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Oracle PeopleSoft Under Siege: Zero-Day CVE-2026-35273 Fuels ShinyHunters Intrusions

Date of Publication	Admiralty Code	TA Number
June 12, 2026	A1	TA2026165

Summary

First Seen: May 27, 2026
Threat Actor: ShinyHunters (aka UNC6240)
Affected Products: Oracle PeopleSoft Enterprise PeopleTools 8.61, 8.62
Impact: CVE-2026-35273 has emerged as a critical zero-day threat targeting Oracle PeopleSoft Enterprise PeopleTools, allowing unauthenticated attackers to remotely take over vulnerable systems. Exploited in the wild by the ShinyHunters (UNC6240) group before a patch was available, the flaw was used to infiltrate organizations, harvest sensitive data, and move laterally across internal networks. The campaign highlights how a single exposed PeopleSoft instance can become the entry point for full-scale enterprise compromise.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-35273	Oracle PeopleSoft PeopleTools Remote Code Execution Vulnerability	Oracle PeopleSoft Enterprise PeopleTools	✓	✗	✓

Vulnerability Details

#1

CVE-2026-35273 is a critical remote code execution (RCE) vulnerability affecting the Updates Environment Management component of Oracle PeopleSoft Enterprise PeopleTools. Classified as CWE-306 (Missing Authentication for Critical Function), the flaw can be exploited remotely over HTTP without requiring any valid credentials. A successful attack allows an unauthenticated threat actor to gain control of a vulnerable PeopleTools instance, potentially leading to a complete system compromise.

#2

Analysis of real-world attacks shows that threat actors are targeting the Environment Management Hub (PSEMHUB) and Integration Broker Listening Connector endpoints. The attack chain leverages Server-Side Request Forgery (SSRF) techniques to bypass access controls by manipulating internal or loopback addresses through request headers and parameters. In some cases, attackers attempt to trigger outbound SMB connections to capture Windows NetNTLM hashes, while persistence can be established by planting malicious XML files that execute through XMLDecoder when the application restarts.

#3

The vulnerability impacts supported PeopleTools versions 8.61 and 8.62, although Oracle has indicated that older, unsupported releases are likely vulnerable as well. Oracle PeopleSoft Enterprise Applications customers may also be affected. Despite the CVSS scope remaining unchanged, the flaw carries severe consequences, with high-impact ratings across confidentiality, integrity, and availability, enabling attackers to fully compromise targeted environments.

#4

Evidence confirms that the vulnerability was actively exploited as a zero-day before Oracle released its June 10, 2026 security alert. The campaign has been linked to the threat actor ShinyHunters (UNC6240), which targeted organizations between May 27 and June 9, 2026. More than 100 organizations were alerted after vulnerable internet-facing systems were identified, with a significant concentration in the higher education sector. While some organizations successfully blocked the attacks, others suffered breaches, and stolen data was later published on the group's data leak site.

#5

Post-exploitation activity reveals a well-organized intrusion operation. The attackers deployed multiple staging servers hosting customized MeshCentral remote management tools disguised as legitimate Microsoft Azure services. Using these systems, they enumerated Oracle PeopleSoft environments, gathered configuration details, mapped internal networks, and moved laterally across compromised infrastructure. Automated scripts were used to spray SSH credentials against internal systems, deploy extortion messages, and collect sensitive data. The stolen information was compressed for exfiltration before being transferred to infrastructure linked to the public ShinyHunters leak site, ultimately supporting the group's extortion and data disclosure operations.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-35273	Oracle PeopleSoft Enterprise PeopleTools (versions 8.61, 8.62)	cpe:2.3:a:oracle:peoplesoft_enterprise_peopletools:*:*:*:*:*:*:*:*	CWE-306

Recommendations

Apply Oracle's Security Alert Without Delay: Install the mitigations and patches referenced in Oracle's Security Alert for CVE-2026-35273 via the PeopleSoft Patch Availability Document immediately. Because this vulnerability is remotely exploitable without authentication and can result in full system takeover, Oracle considers remediation a high-priority risk reduction measure and strongly recommends immediate action. Remain on actively supported PeopleTools versions and apply all Critical Patch Updates, Critical Security Patch Updates, and Security Alerts as they are released.

Disable or Remove the Environment Management Hub: Disable the Environment Management Hub (EMHub) service in multi-server configurations, or completely remove the `PSEMHUB` application in single-server configurations, as advised by Oracle's guidance. Restricting these endpoints is non-breaking for standard end-user operations, since EMHub and the Integration Broker Listening Connector are administrative or system-to-system components not required for core user-facing PeopleSoft Internet Architecture browser sessions.

Restrict Access to Sensitive Endpoints: If you cannot disable the EMHub service, block external network access to `/PSEMHUB/ ` (specifically `/PSEMHUB/hub`) and `/PSIGW/HttpListeningConnector` at the network perimeter or firewall level. Do not rely solely on Web Application Firewall body-inspection rules, as these controls can be bypassed.

Monitor Logs and Network Telemetry: Audit PIA WebLogic access logs for HTTP `POST` requests to `/PSEMHUB/hub` and `/PSIGW/HttpListeningConnector` originating from external or untrusted source IPs. Analyze requests to the listening connector for loopback addresses (`127.0.0.1`, `localhost`, `::1`) or internal IP ranges in headers or parameters, which signal SSRF abuse. Monitor outbound firewall logs and NetFlow data for outbound SMB traffic (TCP port 445) from PeopleSoft hosts to untrusted external destinations, which may indicate attempts to capture NetNTLM hashes.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.004: Unix Shell
Defense Evasion	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
Discovery	T1018: Remote System Discovery	
	T1083: File and Directory Discovery	
Lateral Movement	T1021: Remote Services	T1021.004: SSH
Command and Control	T1219: Remote Access Software	
	T1071: Application Layer Protocol	T1071.001: Web Protocols
Collection	T1560: Archive Collected Data	T1560.001: Archive via Utility

Tactic	Technique	Sub-technique
Exfiltration	T1048: Exfiltration Over Alternative Protocol	
Impact	T1491: Defacement	T1491.001: Internal Defacement
	T1657: Financial Theft	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	142[.]11[.]200[.]186, 142[.]11[.]200[.]187, 142[.]11[.]200[.]188, 142[.]11[.]200[.]189, 142[.]11[.]200[.]190
Domain	azurenetfiles[.]net
SHA256	2ab684d93c1553fad87041b4dea97188a97e78589deee2a7bacff905564f3a35, f02a924c9ff92a8780ce812511341182c6b509d45bc59f3f7b522e37225d24fc, d83fdb9e53c5ff03c4cb0451ea1bebd79b53f29eadc1e2fa394c7af13a86ce2f, c7e9332731b06644fc73e0046a2a89eaa59b09f54250e9bd622467187351711f, 68257a6f9ff196179ec03624e849927f26599eb180a7c82e14ef5bc4e93bc309
Filenames	.bash_history, meshagent32-azure-ops.exe, meshagent64-azure-ops.exe, meshagent64-v2.exe, meshagent, README-IF-YOU-SEE-THIS-YOUVE-BEEN-HACKED.TXT, [victim_abbreviation]_fanout.sh

Patch Links

https://www.oracle.com/security-alerts/alert-cve-2026-35273.html

https://git.kernel.org/pub/scm/linux/kernel/git/stable/linux.git/commit/?id=bbb5d8746381c82f7e0fb6171094d375b492f266

References

https://www.oracle.com/security-alerts/alert-cve-2026-35273.html

https://cloud.google.com/blog/topics/threat-intelligence/shinyhunters-targets-education-sector-oracle-exploit

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a Demo of **HivePro**.

REPORT GENERATED ON

June 12, 2026 • 09:00 AM

More at www.hivepro.com