

HiveForce Labs

THREAT ADVISORY



ATTACK REPORT

From Zero-Day to N-Day: ShinyHunters Renews Oracle PeopleSoft Mass Exploitation

Date of Publication

September 29, 2026

Admiralty Code

A1

TA Number

TA2026287

Summary

First Seen: September 2026

Targeted Regions: Worldwide

Targeted Products: Oracle PeopleSoft

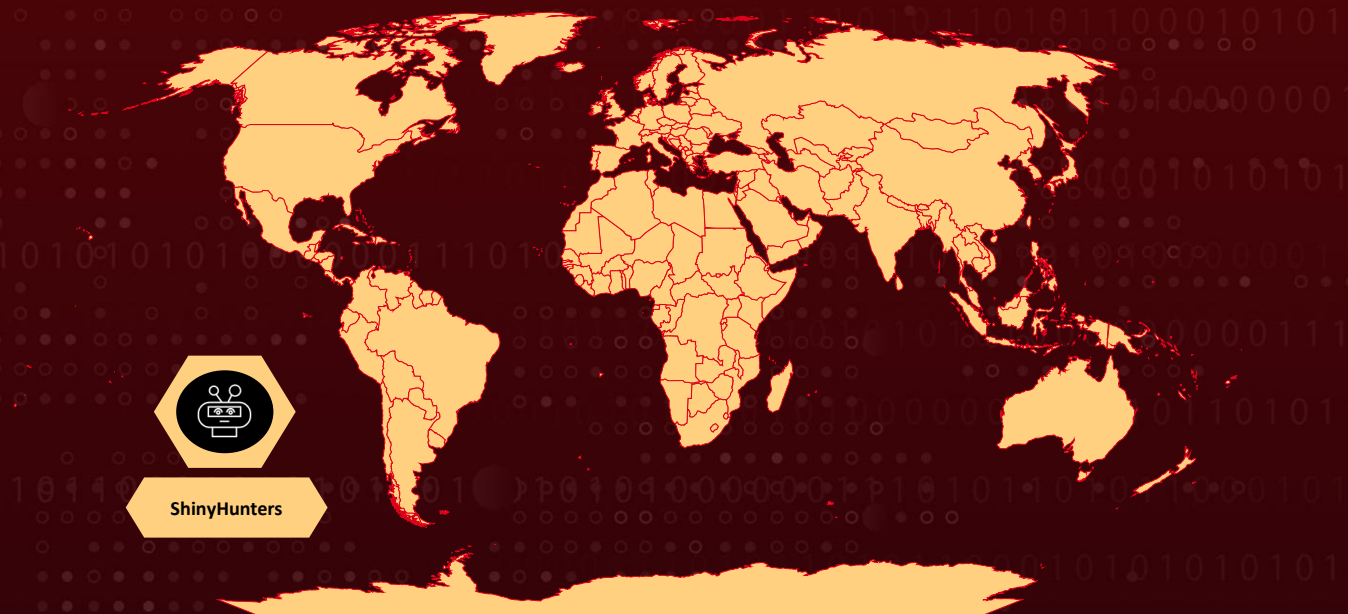
Targeted Industries: Higher education, technology, IT services, healthcare, agriculture, transportation, government

Threat Actor: ShinyHunters (aka UNC6240)

Malware: SIDEEYE backdoor

Attack: ShinyHunters (UNC6240) has renewed mass exploitation of the critical Oracle PeopleSoft PeopleTools flaw CVE-2026-35273. It bypasses WAF rules by URL-encoding a single character in the PSEMHUB path, reaching systems that were never patched. The group has deployed web shells, the SIDEEYE backdoor, Neo-reGeorg tunnels and MeshAgent across higher education, healthcare, government and other sectors worldwide to support data theft and extortion, so organizations must patch immediately and not rely on WAF rules.

🔪 Attack Regions



Targeted

Non-Targeted



THREAT ADVISORY • ATTACK REPORT (Red)

2

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Foundation, TomTom, Zenrin
Hive Pro

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-35273	Oracle PeopleSoft Enterprise PeopleTools Missing Authentication for Critical Function Vulnerability	Oracle PeopleSoft Enterprise PeopleTools			

Attack Details

#1

ShinyHunters (UNC6240) has launched a renewed mass exploitation campaign against Oracle PeopleSoft Enterprise PeopleTools, weaponizing CVE-2026-35273, a critical unauthenticated remote code execution flaw in the Environment Management Hub (PSEMHUB) servlet, patched in June 2026. Having abused the flaw as a zero-day between May 27 and June 9, 2026, predominantly against higher education institutions, the group has now returned with a modified exploit aimed squarely at organizations that relied on web application firewall rules instead of patching.

#2

The bypass is deceptively simple: the attacker URL-encodes a single character, requesting `/%50SEMHUB/` in place of `/PSEMHUB/`. String-based WAF and reverse proxy rules that match the literal path before decoding fail to trigger, while the WebLogic application server decodes the request and routes it to the vulnerable servlet. Targets are first quietly validated through a handful of POST requests carrying a serialized Java object, after which exploitation proceeds via Java deserialization, either planting JSP web shells across every load-balanced node or executing commands filelessly with output returned directly in the HTTP response.

#3

Post-exploitation tooling has matured considerably. Operators deploy paired single-line web shells for hex-encoded command execution and chunked file staging, drop a trojanized, EV-signed media player installer that loads the SIDEYE C++ backdoor in memory for credential theft and reverse proxying, tunnel SOCKS5 traffic through Neo-reGeorg, and maintain persistence through MeshAgent linked to IT-themed infrastructure. A quarter of observed commands ran as root or SYSTEM.

#4

Web shells have been observed on dozens of systems globally across higher education, technology, IT services, healthcare, agriculture, transportation, and government, consistent with the group's established data theft and extortion model. Separately, ShinyHunters claims to have breached FBIJobs.gov using an undisclosed PeopleSoft zero-day; the FBI is investigating but has not determined the point of breach, and no link to CVE-2026-35273 has been established.

Recommendations



Patch Oracle PeopleSoft for CVE-2026-35273: Apply the emergency out-of-band security update for CVE-2026-35273 immediately and remain on actively supported PeopleTools versions; WAF rules and path-based blocking are not a substitute for patching, as the current wave specifically targets unpatched systems sitting behind WAFs.



Disable or Remove the Environment Management Hub: In multi-server configurations disable the EMHub service, and in single-server configurations remove the PSEMHUB application entirely; EMHub and the Integration Broker listening connector are administrative, system-to-system components, so restricting them from the public internet is non-breaking for standard PIA user sessions.



Block the Normalized PSEMHUB Path, Not Literal Strings: Enforce blocking on the normalized request path and assume that any percent-encoded, mixed-case, or otherwise non-normalized variant of /PSEMHUB/ (for example /%50SEMHUB/) may be used; ensure perimeter and proxy rules decode the path before matching.



Hunt Web Shells and the Trojanized Binary Across All Nodes: Inspect <PS_CFG_HOME>/webserv/<domain>/applications/peoplesoft/PSEMHUB.war/ and PORTAL.war/ on every WebLogic node for unexpected .jsp, .jspx, and .exe files, including x.jsp, u.jsp, u2.jsp, tunnel.jsp, tunneljspx, and Ple64.exe, and examine .../PSEMHUB.war/envmetadata/transactions/ for unauthorized content.



Rotate All Credentials Reachable from the Web Tier: Treat any host with a web shell as compromised and rotate credentials readable by the PeopleSoft service account, including database connection strings in psappsrv.cfg, Integration Broker credentials, and any cloud credentials reachable from the web tier, prioritizing hosts where WebLogic runs as root or SYSTEM.



Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Reconnaissance	T1595 : Active Scanning	T1595.002 : Vulnerability Scanning
	T1596 : Search Open Technical Databases	T1596.003 : Digital Certificates
		T1596.005 : Scan Databases
Initial Access	T1190 : Exploit Public-Facing Application	
Execution	T1059 : Command and Scripting Interpreter	T1059.003 : Windows Command Shell
		T1059.004 : Unix Shell
Persistence	T1505 : Server Software Component	T1505.003 : Web Shell
Defense Evasion	T1027 : Obfuscated Files or Information	
	T1140 : Deobfuscate/Decode Files or Information	
	T1553 : Subvert Trust Controls	T1553.002 : Code Signing
Credential Access	T1552 : Unsecured Credentials	T1552.001 : Credentials In Files
	T1110 : Brute Force	T1110.003 : Password Spraying
	T1555 : Credentials from Password Stores	T1555.003 : Credentials from Web Browsers

Tactic	Technique	Sub-technique
Discovery	<u>T1082</u> : System Information Discovery	
	<u>T1016</u> : System Network Configuration Discovery	
Lateral Movement	<u>T1021</u> : Remote Services	<u>T1021.004</u> : SSH
Command and Control	<u>T1105</u> : Ingress Tool Transfer	
	<u>T1071</u> : Application Layer Protocol	<u>T1071.001</u> : Web Protocols
	<u>T1572</u> : Protocol Tunneling	
	<u>T1090</u> : Proxy	
	<u>T1219</u> : Remote Access Software	
Collection	<u>T1560</u> : Archive Collected Data	<u>T1560.001</u> : Archive via Utility
Exfiltration	<u>T1048</u> : Exfiltration Over Alternative Protocol	
Impact	<u>T1491</u> : Defacement	<u>T1491.001</u> : Internal Defacement

✂ Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	48b4a0827da7bbfce9fb52464f8a659dea7a035189c52c506c0bfb4b1c3fe494, 2bee941fb40519d0d1ec52bd79a8f63fc65aac6455c8f2d6b668e3360dfdb5d7, 419c571ee38b7e7266d130c4b6bbbc4dd0ef44d6e5f3bc02cc2cf73b762f07c86, ba14419beb2ec0bb94cab6298c14d7fb3e1d819366fe378290c0c2a4d97f7e07, 3ba215692665513abfffd4e815c5c45f2d41e5dcc4283a2a3b740930c5c417c3, 2ab684d93c1553fad87041b4dea97188a97e78589deee2a7bacff905564f3a35, f02a924c9ff92a8780ce812511341182c6b509d45bc59f3f7b522e37225d24fc, d83fdb9e53c5ff03c4cb0451ea1bebd79b53f29eadc1e2fa394c7af13a86ce2f, c7e9332731b06644fc73e0046a2a89eaa59b09f54250e9bd622467187351711f, 68257a6f9ff196179ec03624e849927f26599eb180a7c82e14ef5bc4e93bc309
IPv4	5[.]199[.]162[.]157, 104[.]219[.]234[.]138, 162[.]219[.]30[.]165, 142[.]11[.]200[.]186, 142[.]11[.]200[.]187, 142[.]11[.]200[.]188, 142[.]11[.]200[.]189, 142[.]11[.]200[.]190, 176[.]120[.]22[.]24
IPv4:Port	162[.]219[.]30[.]165[:]:3333, 162[.]219[.]30[.]165[:]:3334

TYPE	VALUE
Domains	winmanage-me[.]network, azurenetafiles[.]net, microsoft-entra[.]net, enroll[.]azuredevice[.]cloud
URL	wss[:]//azurenetafiles[.]net[:]443/agent[.]ashx
Filename	x.jsp, u.jsp, u2.jsp, tunnel.jsp, tunnel.aspx, Ple64.exe, README-IF-YOU-SEE-THIS-YOUE-BEEN-HACKED.TXT, [victim_abbreviation]_fanout.sh, meshagent, meshagent.msh, meshagent.db, meshagent32-azure-ops.exe, meshagent64-azure-ops.exe, meshagent64-v2.exe
File Path	<PS_CFG_HOME>/webserv/<domain>/applications/peoplesoft/PSEM HUB.war/x.jsp, <PS_CFG_HOME>/webserv/<domain>/applications/peoplesoft/PSEM HUB.war/u.jsp, <PS_CFG_HOME>/webserv/<domain>/applications/peoplesoft/PSEM HUB.war/Ple64.exe, <PS_CFG_HOME>/webserv/<domain>/applications/peoplesoft/PSEM HUB.war/tunnel.jsp, <PS_CFG_HOME>/webserv/<domain>/applications/peoplesoft/PSEM HUB.war/tunnel.aspx
HTTP Request	/%50SEMHUB/ GET /%50SEMHUB/<webshell>.jsp?c=id;hostname;uname+-a



Patch Link

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



References

<https://cloud.google.com/blog/topics/threat-intelligence/shinyhunters-renewed-mass-exploitation-campaign-targeting-oracle-peoplesoft>

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

<https://www.hivepro.com/threat-advisory/oracle-peoplesoft-under-siege-zero-day-cve-2026-35273-fuels-shinyhunters-intrusions>

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

September 29, 2026 • 07:30 AM

© 2026 All Rights are Reserved by Hive Pro



More at www.hivepro.com