Oracle PeopleSoft Zero-Day Actively Exploited in Data Theft Attacks

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

A critical vulnerability in PeopleSoft PeopleTools (CVE-2026-35273, CVSS 9.8) is being actively exploited. The flaw may allow an unauthenticated attacker to compromise affected systems and steal sensitive data.

Overview

There is a critical vulnerability (CVE-2026-35273, CVSS 9.8) in Oracle PeopleSoft PeopleTools, a component of Oracle PeopleSoft used by organizations to manage business functions such as human resources, payroll, finance, and student information.

The vulnerability is missing an authentication flaw and allows an unauthenticated attacker with network access via HTTP to compromise vulnerable PeopleSoft environments. Successful exploitation can result in complete takeover of affected PeopleTools instances.

Affected Products

- Oracle PeopleSoft PeopleTools 8.61
- Oracle PeopleSoft PeopleTools 8.62
- Oracle PeopleSoft Enterprise Applications may also be affected

CVE-2026-35273 has been added to CISA's Known Exploited Vulnerabilities (KEV) Catalog and is being actively exploited. Exploitation has been linked to the ShinyHunters data theft and extortion group. Researchers believe more than 100 organizations may have been impacted, including a significant number in the higher education sector.

Because PeopleSoft often contains sensitive business and personal information and is commonly integrated with other enterprise systems, successful exploitation could provide access to sensitive employee, student, and financial data stored within PeopleSoft environments.

Aspire Protects

- **Patch** - Oracle issued a Security Alert and provided mitigations/workarounds for customers running affected versions of PeopleSoft PeopleTools 8.61 and 8.62 while a patch is being developed.
- Review PeopleSoft, WebLogic, web server, and authentication logs for suspicious requests targeting `/PSEMHUB/` and `/PSIGW/HttpListeningConnector`.
- Inspect systems for JSP webshells, unauthorized files, suspicious directories, and recently modified XML files.

TTPs

Initial Access

- Exploit Public-Facing Application (T1190) – Exploitation of a vulnerable internet-facing PeopleSoft instance may allow unauthorized access to the environment.

Discovery

- System Information Discovery (T1082) – Access to a compromised PeopleSoft environment may allow attackers to gather information about PeopleSoft, WebLogic, and connected systems.

Lateral Movement

- Valid Accounts (T1078) – Stolen or compromised credentials may be used to access additional systems and expand access within the environment.

Collection

- Data from Information Repositories (T1213) – Sensitive employee, student, financial, or operational data stored within PeopleSoft environments may be accessed and collected.

IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Organizations using Oracle PeopleSoft may be affected, especially those in:

- Higher Education
- Healthcare
- Public Sector
- Finance

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Oracle Security Alert Advisory - CVE-2026-35273

Known Exploited Vulnerabilities Catalog | CISA