Smarttech
YOUR 24/7 SECURITY PARTNER

Oracle PeopleSoft Vulnerability Actively Exploited – 12th June 2026

Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	102
Authors	Dorin Constantin Banu < constatin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-06-12
Issue Date	2026-06-11

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

A critical vulnerability in Oracle PeopleSoft is being actively exploited in the wild. Tracked as CVE-2026-35273, the flaw stems from a weakness in the Updates Environment Management component that exposes management functionality over HTTP without authentication, allowing remote code execution. Once inside, attackers deploy backdoors, perform lateral movement, and exfiltrate sensitive data. The campaign impacted over 100 organizations and approximately 300 PeopleSoft instances, predominantly affecting universities.

Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **Critical**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **Critical**

Technical summary

More details related to this vulnerability are as follows:

CVE ID	Description
CVE-2026-35273 **CVSS Base Score: 9.8**	An unauthenticated attacker with network access via HTTP can execute arbitrary code and fully compromise affected PeopleSoft Enterprise PeopleTools instances.

Affected Products

- PeopleSoft Enterprise PeopleTools, versions 8.61, 8.62
- Earlier, unsupported versions may also be affected

Identifying an attack

- WebLogic access logs showing external POST requests to /PSEMHUB/hub or /PSIGW/HttpListeningConnector.

- Unexpected .jsp files under the PSEMHUB.war web application directory, or odd folders named logs, persistantstorage, or scratchpad under the PSEMHUB paths.
- Recently changed .xml files under the web doc root's envmetadata/data/environment, which can be abused for XMLDecoder persistence that fires on the next restart.
- Outbound SMB traffic on port 445 from PeopleSoft hosts to external destinations, which the exploit chain may use to capture machine-account NetNTLM hashes.

Mitigation

- Disable the Environment Management Hub service on multi-server setups or remove the PSEMHUB application outright on single-server setups.
- If these are not an option, then block external access to /PSEMHUB/* (especially /PSEMHUB/hub) and /PSIGW/HttpListeningConnector at the perimeter.

Note: WAF body-inspection rules alone are not enough, since they can be bypassed. Restricting these endpoints does not break normal user sessions.

Recommendations

Smarttech247 team recommend the following actions be taken:

- Apply the appropriate patches, hotfixes or appropriate mitigations provided by Oracle to vulnerable systems immediately after appropriate testing.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner for prevention.
- Use the right Vulnerability Management Tools to assess endpoint, networks or applications for known weaknesses.
- Apply the Principle of Least Privilege to all systems and services.
- Apply advanced application control and protection to enforce granular control over all application access, communications, and privilege elevation attempts.
- Kindly ensure that your Endpoint Security and Perimeter security products are updated with the latest signatures to detect these threats.

References

https://thehackernews.com/2026/06/shinyhunters-exploits-oracle-peoplesoft.html?m=1
https://www.oracle.com/security-alerts/alert-cve-2026-35273.html
https://www.securityweek.com/oracle-addresses-peoplesoft-vulnerability-amid-reports-of-zero-day-attacks/

CVE

CVE-2026-35273

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com