CYBER ADVISORY

Friday, June 12, 2026 **CAL-CSIC-202606-A-009**

Critical Vulnerability Under Active Exploitation Impacting Oracle PeopleSoft Enterprise PeopleTools

Remote Code Execution	Unauthenticated Attacker	Under Active Exploitation	Patch Available

The Cybersecurity Integration Center (CSIC) has become aware of a critical vulnerability impacting Oracle's PeopleSoft Enterprise PeopleTools development framework. CVE-2026-35273 carries a CVSS 3.1 score of 9.8.[1] The vulnerability enables an unauthenticated attacker with network access via HTTP to compromise the platform. Successful exploitation would allow remote code execution and *complete takeover* of PeopleSoft Enterprise PeopleTools.[2] The vulnerability requires no user interaction and highly impacts CIA.

As of June 10, 2026, Oracle has issued a Security Alert Advisory and considers this vulnerability to be a high-priority risk. Oracle clients who implement PeopleSoft Enterprise PeopleTools are strongly encouraged to take immediate action to address the vulnerability.[3] Current open-source reporting indicates that this vulnerability is currently being exploited by threat actor group "ShinyHunters". The group is claiming to have compromised more than 100 organizations and have exfiltrated data from close to 300 PeopleSoft instances.[4] This claim is further substantiated due to Mandiant and Google Threat Intelligence Groups identification of an active compromise and extortion campaign attributed to the same threat actor group observed between May 27-June 9 2026 – effectively exploited as a zero-day vulnerability.[5]

The Cal-CSIC recommends following Oracle's mitigation guidance as soon as possible. Please note that an Oracle login is required regarding patch availability. For additional details regarding Security Alert Supported Products and Versions for CVE-2026-35273, please use this link:

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

Affected Product(s) and Version(s)

Product	Affected Version
PeopleSoft Enterprise PeopleTools	8.61, 8.62

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] NVD; "CVE-2026-35273 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-35273; accessed 12 June 2026
[2] Tenable; "CVE-2026-35273"; https://www.tenable.com/cve/CVE-2026-35273; accessed 12 June 2026
[3] Oracle; "Oracle Security Alert Advisory – CVE-2026-35273"; https://www.oracle.com/security-alerts/alert-cve-2026-35273.html; accessed 12 June 2026
[4] TechRadar; "Oracle warns customers of critical PeopleSoft attack after hundreds of servers hacked by apparent ShinyHunters data theft attacks"; https://www.techradar.com/pro/security/oracle-warns-customers-of-critical-peoplesoft-attack-after-hundreds-of-servers-hacked-by-apparent-shinyhunters-data-theft-attacks; accessed 12 June 2026
[5] Google Cloud Blog; "ShinyHunters Targets Education Sector with Oracle PeopleSoft Exploit"; https://cloud.google.com/blog/topics/threat-intelligence/shinyhunters-targets-education-sector-oracle-exploit; accessed 12 June 2026