Exploited Oracle PeopleSoft Zero-Day Is Three Chained Flaws, Patched Under CVE-2026-35273



Researchers say the critical PeopleSoft bug exploited by ShinyHunters since May is three chained flaws. Oracle fixed all three in June under CVE-2026-35273; the root is an SSRF reaching an internal management interface.

- The PeopleSoft flaw exploited by ShinyHunters since May is three vulnerabilities chained together, not one.
- Oracle patched all three in June under a single identifier, CVE-2026-35273.
- The root is a server-side request forgery (SSRF) that reaches an internal management interface.
- The SSRF works because PeopleSoft trusts its own loopback address.

Researchers who reported the critical Oracle PeopleSoft vulnerability exploited by ShinyHunters have clarified

that it is not a single flaw. It consists of three flaws chained together, and the group has been exploiting it since May.

What is known

Oracle addressed all three issues in June under one identifier, **CVE-2026-35273**. The chain begins with a server-side request forgery (SSRF). Through it, an attacker can reach an internal management interface, because PeopleSoft trusts requests that appear to come from its own loopback address.

The source does not describe the other two flaws, the affected versions, or the data accessed, so we do not speculate on them.

Why it matters

Because the chain was exploited from May and fixed in June, systems may have been exposed before patching. Institutions running PeopleSoft should treat patch status and a review of past activity as separate questions: applying the update closes the path, but it does not show whether it was used earlier.

Recommended approach

Confirm that the June Oracle update covering CVE-2026-35273 is installed on every PeopleSoft environment, including test and disaster recovery systems. Then review logs for the period since May for unusual requests to internal interfaces.

What to do now

1. Verify the June Oracle update for CVE-2026-35273 is applied on all PeopleSoft environments, including test and DR.
2. Review PeopleSoft web and application logs from May onward for unusual requests to internal management interfaces.
3. Restrict access to PeopleSoft management interfaces to approved administrative networks only.
4. If suspicious activity is found, start incident response and assess notification duties under PDPL and sector regulators.