

Home • Security • Vulnerabilities



by **Evan Schuman**
Contributor

Despite ShinyHunters arrests after FBI jobs data breach, enterprises still have no answers about PeopleSoft risks

News

Oct 5, 2026 • 5 mins

One prominent analyst recommends that PeopleSoft customers pull the Environment Management Hub and the Integration Broker off the public internet.



Credit: Kristi Blokhin / Shutterstock [<https://enterprise.shutterstock.com/image-photo/washington-dc-usa-december-29-2016-555190222>]

The theft of FBI employee data by hacking group ShinyHunters, and the subsequent shutdown of the FBI's **Peoplesoft-based jobs portal** [<https://web.archive.org/web/20260922144902/https://fbijobs.gov/>], is causing concern for enterprise users of the Oracle product, with analysts recommending extreme measures in response.

Law enforcement has made some progress in its pursuit of the cyber criminals involved, but there has still been no official word from either the FBI or Oracle about Peoplesoft's alleged involvement.

On Saturday, Reuters reported that a suspected member of ShinyHunters **had been arrested** [<https://www.reuters.com/world/middle-east/key-shinyhunters-hacker-detained-jordan-is-cooperating-sources-say-2026-10-03/>] in Jordan and has been cooperating with law enforcement to help identify other member of the group. The arrest comes a week after the **arrest of another suspected ShinyHunters member by the Dutch National Police** [<https://www.fbi.gov/video-repository/shinyhunters-arrested-092926.mp4/view>]. In a video about that arrest, an FBI official warned gang members that arrests have a way of changing who is willing to talk, concluding, "You know how to find us, and we know how to find you." Before the arrests, the gang told The Register it had discovered a new PeopleSoft zero-day hole and leveraged it to break into an FBI system, stealing information on all FBI employees. The **FBI has since confirmed the breach** [<https://www.fbi.gov/news/press-releases/fbi-statement-on-compromise-of-fbijobs.gov-portal-and-alleged-impact-to-fbi-employee-pii>] without providing details.

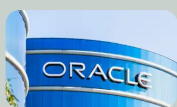
This wouldn't be the first flaw ShinyHunters had found in PeopleSoft. It discovered a PeopleSoft zero-day hole in June that **resulted in a flurry of extortion attempts** [<https://www.csoononline.com/article/4184408/oracle-peoplesoft-zero-day-fuels-shinyhunters-extortion-spree.html>], long after **Oracle said it had patched the bugs** [<https://www.csoononline.com/article/4200184/oracles-july-update-fixes-ten-10-0-vulnerabilities-in-fusion-middleware.html>].

Oracle did not respond to a request for comment on the alleged new vulnerability.

Significant risk exposure for enterprises

Analysts and consultants played up the risk exposure from the potentially new vulnerability even as they sharply played down the implications of the arrest.

Recommended for you



Oracle releases 245 new security patches, all rated 'high-priority security'

By Evan Schuman

• 6 mins

[https://www.csoononline.com/?post_type=post&p=4186983&utm_source=miso&utm_medium=related&utm_campaign=thumb_nail_list]



Overly permissive
'guest' settings put
Salesforce
customers at risk
By Shweta Sharma • 4 mins

[https://www.csoononline.com/?post_type=post&p=4143667&utm_source=miso&utm_medium=related&utm_campaign=thumbnail_list]



AI finds so many
Windows flaws,
Microsoft can't
keep up. Should
you worry?
By Preston Gralla • 6 mins

[https://www.computerworld.com/?post_type=post&p=4207441&utm_source=miso&utm_medium=related&utm_campaign=thumbnail_list]

Frank Dickson [<https://www.linkedin.com/in/frankdickson/>], principal analyst at Dickson Research, recommended that PeopleSoft users take immediate action.

"If it is a new flaw, the patch is necessary but not sufficient. PeopleSoft customers should pull the Environment Management Hub and the Integration Broker off the public internet," he said. "Doing so does not break normal user sessions."

He also encouraged users to quickly implement many of **the recommendations** [<https://cloud.google.com/blog/topics/threat-intelligence/shinyhunters-renewed-mass-exploitation-campaign-targeting-oracle-peoplesoft>] from Google unit Mandiant's report late last month on PeopleSoft security issues, especially "hunting for the web shells and outbound traffic Mandiant describes."

"For PeopleSoft shops, the to-do list is short," Dickson said. "Apply Oracle's patch. Disable or remove the Environment Management Hub if you do not use it. Search your logs for encoded variants of the PSEMHUB path, not just the literal string. If you find a web shell, treat the server as compromised and rotate every credential it could read."

CSO Smart Answers [Learn more](#)

Explore related questions

- [How do attackers hide malware inside an Oracle Database?](#)
- [Why are deserialization vulnerabilities considered a major threat to system security?](#)
- [Can cloud security models truly guarantee tenant isolation and data protection?](#)
- [Why have ERP systems become the primary target for modern cyberattacks?](#)
- [What should I know about Oracle's high-priority security patch updates?](#)

This is a dangerous situation, he said: “An unpatched PeopleSoft flaw is a Sword of Damocles over every PeopleSoft shop

But despite the extreme risk, even after the patch was released, rather than applying it, some organizations have opted for other mitigations. “Many organizations chose to block the vulnerable endpoint with web application firewall rules rather than patch,” Dickson said. “The attackers walked past those rules by changing a single character in the web address, writing ‘%50’ in place of the letter ‘P.’”

Could signal a bigger problem

However, IDC Research Director **Philip Harris** [<https://my.idc.com/getdoc.jsp?containerId=PRF005506>] encouraged CISOs to view the FBI’s confirmation of its breach with caution, given the attack vector was not revealed.

“ShinyHunters says it used a second, previously undocumented PeopleSoft preauth RCE zero-day, distinct from the CVE-2026-35273 flaw exploited in the earlier campaign,” he said. Yet, he pointed out, “no CVE has been assigned to it, it has not appeared on CISA’s Known Exploited Vulnerabilities catalog and Oracle has not commented on it. Every outlet covering this is explicit that the zero-day claim comes only from the threat actor, not from independent forensic confirmation or from Oracle. That distinction matters.”

But if the hole is as the group has suggested, Harris said it signals a much bigger problem.

“Assuming it is real, this would mean PeopleSoft has a second critical, unpatched preauth RCE in the same window as CVE-2026-35273, a pattern of recurring critical exposure rather than one isolated bug,” he said. “ShinyHunters’ own claim that they are already using it against other, unnamed Fortune 500 targets would mean every PeopleSoft customer is currently exposed to an unpatchable, undisclosed flaw with no vendor guidance to act on, a meaningfully worse position than the WAF-bypass story, since there is no mitigation to attempt while waiting on Oracle to confirm something it has not acknowledged.”

Jeff Valdes [<https://acceligence.com/talent/profiles/jeff-valdes/>], a director at consulting firm Acceligence, added that Oracle’s silence is unwarranted.

“I think customers reasonably want more communication from the vendor,” he said. “They want to understand whether Oracle’s original guidance remains sufficient, whether there are additional mitigations customers should implement, whether Oracle is seeing anything through its own support organization that changes the risk picture, and whether there are configurations or architectural choices that materially increase exposure. Those are operational security questions that can be addressed without discussing attribution,

arrests, investigative techniques or anything else that might interfere with an FBI investigation.”

[Vulnerabilities\[https://www.csoonline.com/vulnerabilities/\]](https://www.csoonline.com/vulnerabilities/)

[Security\[https://www.csoonline.com/security/\]](https://www.csoonline.com/security/)

[Enterprise\[https://www.csoonline.com/enterprise/\]](https://www.csoonline.com/enterprise/)

[Business\[https://www.csoonline.com/business/\]](https://www.csoonline.com/business/)

[Industry\[https://www.csoonline.com/industry/\]](https://www.csoonline.com/industry/)

[Zero-Day Vulnerabilities\[https://www.csoonline.com/zero-day-vulnerabilities/\]](https://www.csoonline.com/zero-day-vulnerabilities/)

NEWSLETTER

Don't miss a thing

Join the CSO First Look mailing list for the latest news, analysis, and insights. Sign up now!

Email Address

☐ By submitting your information, you agree to our [PRIVACY POLICY \[https://foundryco.com/privacy-policy/\]](https://foundryco.com/privacy-policy/).

Subscribe

About

- About Us
- Advertise
- Contact Us
- Editorial ethics policy
- Foundry Careers
- Reprints
- Newsletters
- Contribute to CSO

Policies

- Terms of Service
- Privacy Policy
- Cookie Policy
- Copyright Notice
- Member Preferences
- About AdChoices
- Your California Privacy Rights

Add CSO as a Preferred Source in Google Search

More

Awards

Blogs

BrandPosts

Events

Podcasts

Videos

Buyer's Guides

Our Network

CIO

Computerworld

InfoWorld

Network World

FOUNDRY



© 2026 FoundryCo, Inc. All Rights Reserved.