ثغرة Oracle PeopleSoft المستغلة هي في الواقع ثلاث ثغرات متسلسلة، وقد عولجت ضمن CVE-2026-35273



أفاد باحثون بأن ثغرة PeopleSoft الحرجة التي استغلتها ShinyHunters منذ مايو هي ثلاث ثغرات متسلسلة. عالجتها Oracle في يونيو ضمن CVE-2026-35273، وأصلها SSRF يصل إلى واجهة إدارة داخلية.

- الثغرة التي استغلتها ShinyHunters في PeopleSoft منذ مايو هي ثلاث ثغرات متسلسلة وليست ثغرة واحدة.
- عالجت Oracle الثغرات الثلاث في يونيو تحت معرّف واحد هو CVE-2026-35273.
- أصل المشكلة هو SSRF يصل إلى واجهة إدارة داخلية.
- ينجح الهجوم لأن PeopleSoft تثق بعنوان الحلقة الراجعة (loopback) الخاص بها.

أوضح الباحثون الذين أبلغوا عن ثغرة Oracle PeopleSoft الحرجة التي تستغلها ShinyHunters أنها ليست ثغرة

واحدة، بل ثلاث ثغرات متسلسلة، وأن المجموعة تستغلها منذ مايو.

ما هو معروف

عالجت Oracle المشكلات الثلاث في يونيو تحت معرّف واحد هو **CVE-2026-35273**. تبدأ السلسلة بثغرة تزوير طلبات من جهة الخادم (SSRF)، يستطيع المهاجم من خلالها الوصول إلى واجهة إدارة داخلية، لأن PeopleSoft تثق بالطلبات التي تبدو صادرة من عنوان الحلقة الراجعة (loopback) الخاص بها.

لا يتناول المصدر الثغرتين الأخريين ولا الإصدارات المتأثرة ولا البيانات التي جرى الوصول إليها، ولذلك لا نفترض شيئاً بشأنها.

أهمية الأمر

بما أن الاستغلال بدأ في مايو وصدر الإصلاح في يونيو، فقد تكون الأنظمة معرضة قبل تطبيق التحديث. على الجهات التي تشغّل PeopleSoft أن تعامل حالة التحديث ومراجعة النشاط السابق كمسألتين منفصلتين: فالتحديث يغلق المسار لكنه لا يبيّن ما إذا استُخدم سابقاً.

النهج الموصى به

تأكدوا من تثبيت تحديث Oracle الصادر في يونيو والخاص بـ CVE-2026-35273 على جميع بيئات PeopleSoft، بما فيها الاختبار والتعافي من الكوارث. ثم راجعوا السجلات منذ مايو بحثاً عن طلبات غير معتادة إلى الواجهات الداخلية.

ما يجب فعله الآن

1. تحقق من تطبيق تحديث Oracle الصادر في يونيو لمعالجة CVE-2026-35273 على جميع بيئات PeopleSoft، بما فيها الاختبار والتعافي من الكوارث.
2. راجع سجلات الويب والتطبيق في PeopleSoft منذ مايو بحثاً عن طلبات غير معتادة إلى واجهات الإدارة الداخلية.
3. اقصر الوصول إلى واجهات إدارة PeopleSoft على شبكات الإدارة المعتمدة فقط.
4. عند رصد نشاط مشبوه، فعّل الاستجابة للحوادث وقيّم متطلبات الإبلاغ بموجب نظام حماية البيانات الشخصية (PDPL) وجهات التنظيم القطاعية.