GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel : (678) 33380

GOUVERNEMENT DE LA RÉPUBLIQUE DE VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICE DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

SPR 9108 Port-Vila, Vanuatu
Tél : (678) 33380

28 octobre 2025

Avis 107 : Vulnérabilité non spécifiée dans Oracle E-Business Suite

Date de publication : 6 octobre 2025
Degré d'impact : ÉLEVÉ / CRITIQUE
TLP : CLAIR

Le service de Communication et de Transformation numérique (SCTN), par l'intermédiaire du CERTVU publient l'avis suivant.

Cette alerte s'adresse aux organisations ainsi qu'aux administrateurs de systèmes et réseaux utilisant les produits mentionnés ci-dessus. Elle est destinée à être comprise par des utilisateurs techniques et administrateurs de systèmes.

Objet de l'alerte

La vulnérabilité **CVE-2025-61882** constitue une faille **critique d'exécution de code à distance (RCE)** en phase de pré-authentification, impactant Oracle E-Business Suite (EBS), et plus particulièrement le composant Oracle Concurrent Processing, intégré à BI Publisher. Cette vulnérabilité permet à un attaquant non authentifié, accessible via HTTP, d'exécuter du code arbitraire sur le serveur ciblé.

En savoir plus

Systèmes concernés

Versions affectées :

- Les instances d'Oracle E-Business Suite exposées à Internet, fonctionnant sous les versions 12.2.3 à 12.2.14, doivent être considérées comme prioritaires pour la mise en œuvre des mesures correctives.

Implications

Comment des attaquants exploitent cette vulnérabilité (vecteur d'attaque).

- À distance, sans authentification, via HTTP : des attaquants envoient des requêtes HTTP spécialement conçues vers le point d'entrée vulnérable de BI Publisher / Concurrent Processing pour déclencher l'exécution de code à distance (RCE).
- Exploitation en conditions réelles / active : plusieurs rapports et fournisseurs de renseignement sur les menaces ont observé des campagnes actives ainsi que la diffusion de scripts d'exploitation associés à cette vulnérabilité.

Mesures d'atténuation

CERTVU recommande :

1. D'appliquer immédiatement les correctifs - Déployer sans délai l'alerte de sécurité d'urgence et les correctifs Oracle relatifs à la vulnérabilité CVE-2025-61882 pour l'ensemble des versions d'EBS concernées.

2. En cas d'impossibilité de mise à jour immédiate :
    - Restreindre l'accès HTTP à EBS, notamment aux points d'entrée Concurrent Processing et BI Publisher, au niveau réseau en limitant l'accès aux adresses IP de confiance et aux connexions VPN uniquement.
    - Implémenter des règles WAF/IPS visant à bloquer les schémas d'attaque inconnus et activer les signatures IDS/fournisseurs associées à cette vulnérabilité.
    - Isoler tout serveur EBS exposé directement à Internet.

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2025-61882
3. https://www.oracle.com/security-alerts/alert-cve-2025-61882.html
4. https://success.trendmicro.com/en-US/solution/KA-0021286