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 REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

10 October 2025

Advisory 107: Oracle E-Business Suite Unspecified Vulnerability

Release Date: 06th of October 2025
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communication and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2025-61882 – is a **critical, pre-authentication remote code execution (RCE)** in Oracle E-Business Suite (EBS) – specifically affecting the Oracle Concurrent Processing component (BI Publisher integration). An unauthenticated attacker reachable over HTTP can exploit the flaw to run arbitrary code on the server.

Read more

What are the Systems affected?

Affected:

- Oracle E-Business Suite 12.2.3 through 12.2.14. Treat any internet-facing EBS instances in these versions as high priority for remediation.

What does this mean?

How attackers exploit this vulnerability (attack vector)

- Remote, unauthenticated HTTP: attackers send specially crafted HTTP request to the vulnerable BI Publisher / Concurrent Processing endpoint to trigger the RCE.
- In the wild / active exploitation: multiple reports and threat-intel vendors have observed active campaigns and leaked exploit script tied to this CVE

Mitigation process

CERTVU recommend:

1. Immediate Patching - Apply Oracle's emergency Security Alert / patches for CVE-2025-61882 for all affected EBS versions.
2. If for some reasons you cannot block immediately:
    - Block/limit HTTP access to EBS (especially the Concurrent Processing / BI Publisher endpoints) at the network parameter – restrict to trusted Ips and VPN only.
    - Apply WAF /IPS Rules to block unknown exploit patterns and enable vendor/IDS signatures the reference this CVE.
    - Isolate any internet-facing EBS host

Reference

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