AL2025_48 Oracle E-Business Suite Zero-Day (CVE-2025-61882) Exploited in Clop Data-Theft Campaign (October 7th, 2025)

Description

Oracle has released an emergency security update to address a critical, unauthenticated remote-code-execution vulnerability in Oracle E-Business Suite (CVE-2025-61882, CVSS 9.8). Threat actors linked to the Clop extortion campaign have exploited this flaw to steal data from vulnerable EBS instances and are sending extortion emails to affected organisations. Oracle advises customers to apply the update immediately; the new patch requires customers to have installed the October 2023 Critical Patch Update before applying the fix.

Attack Details

- CVE-2025-61882 affects Oracle Concurrent Processing (BI Publisher Integration) in Oracle E-Business Suite versions **12.2.3–12.2.14** and allows unauthenticated RCE over HTTP.
- Oracle published indicators of compromise (IOCs) tied to observed exploitation, including two IP addresses (200[.]107[.]207[.]26 and 185[.]181[.]60[.]11), a reverse-shell command, and exploit archive files posted publicly.
- Exploit code and a related archive (e.g., oracle_ebs_nday_exploit_poc_scattered_lapsus_retard_cl0p_hunters.zip) were leaked by other threat actors and correspond to Oracle's IOCs.
- Clop (and possibly associated extortion actors) have begun contacting organisations with ransom demands claiming EBS data theft. Investigations are ongoing and some activity appears linked to previously patched July 2025 vulnerabilities as well.

Remediation

- **Apply Oracle's Emergency Update Immediately:** Follow Oracle's Security Alert for **CVE-2025-61882** and install the provided EBS patches. Ensure the October 2023 Critical Patch Update is installed first if required.
- **Isolate & Patch Exposed Systems:** If you host internet-facing EBS instances, isolate them, apply patches, and remove direct public access where feasible (use VPNs/bastion hosts and allow-lists).
- **Search for IOCs & Signs of Compromise:** Look for connections from the listed IPs, the reverse-shell command pattern (/bin/bash -i >& /dev/tcp/...), presence of exploit archive files or

unexpected web requests, and any unusual command execution or webshells. Preserve logs and forensic evidence.

- **Review Authentication & Credentials:** Rotate any exposed credentials, review account activity and privileged access, and enforce strong authentication (MFA) for EBS administrative accounts.
- **Hunt for Data Theft Indicators:** Look for large exports, unusual downloads, or exfiltration to unknown hosts; treat extortion emails as high-risk intelligence and correlate with your logs.
- **Notify & Coordinate:** If you suspect compromise, preserve evidence, follow your incident response plan, and notify legal/compliance and CIRT.GY. Engage forensic/IR specialists as needed.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Abrams, L. (2025, October 5). Oracle patches EBS zero-day exploited in Clop data theft attacks. BleepingComputer. Retrieved from https://www.bleepingcomputer.com/news/security/oracle-patches-ebs-zero-day-exploited-in-clop-data-theft-attacks/

- Oracle. (2025, October 4). Security Alert — CVE-2025-61882 (Oracle E-Business Suite). Oracle Security Alerts. Retrieved from https://www.oracle.com/security-alerts/alert-cve-2025-61882.html