Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

CVE-2025-61882: Oracle EBS Zero-Day Actively Exploited in the Wild

Date of Publication	Admiralty Code	TA Number
October 8, 2025	A1	TA2025307

Summary

First Seen: August 9, 2025
Affected Product: Oracle E-Business Suite
Threat Actor: Scattered Spider, ShinyHunters, and LAPSUS$
Malware: Cl0p Ransomware
Impact: CVE-2025-61882 is a critical unauthenticated remote code execution flaw in Oracle E-Business Suite (EBS) BI Publisher Integration, affecting versions 12.2.3–12.2.14 with a CVSS score of 9.8. Exploited via crafted HTTP requests and malicious XSLT uploads, it enables full system compromise. Actively used by the Cl0p ransomware group since August 2025, exploitation surged after an October 2025 proof-of-concept leak by the "Scattered Lapsus$ Hunters" collective.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-61882	Oracle E-Business Suite Unspecified Vulnerability	Oracle E-Business Suite	✓	✓	✓

Vulnerability Details

#1

CVE-2025-61882 is a critical remote code execution vulnerability affecting Oracle E-Business Suite (EBS), specifically the Concurrent Processing component through its BI Publisher Integration. The flaw allows unauthenticated attackers to execute arbitrary code over HTTP, enabling full system compromise, credential theft, data exfiltration, and disruption of enterprise operations across financial, HR, and supply chain functions. Affecting Oracle EBS versions 12.2.3 through 12.2.14, the vulnerability holds a CVSS 3.1 score of 9.8, underscoring its severity and ease of exploitation.

#2

Technically, the attack chain involves sending crafted HTTP POST requests to specific Oracle EBS endpoints to bypass authentication. Attackers then upload malicious XSLT templates that, when processed by the BI Publisher engine, result in arbitrary command execution on the underlying Java web server. Compromised systems often establish outbound HTTPS connections over port 443 to attacker-controlled infrastructure, enabling persistence, lateral movement, and further exploitation.

#3

The simplicity of the exploit, combined with the widespread internet exposure of Oracle EBS systems, has led to automated mass scanning and opportunistic targeting that often evades traditional network defenses. Active exploitation has been ongoing since at least August 2025, led by the Cl0p ransomware group in campaigns involving data theft and double extortion. Indicators of compromise include unauthorized web shells, outbound C2 traffic, and stolen application credentials.

#4

In early October 2025, a public proof-of-concept exploit was leaked by a threat actor coalition known as “Scattered Lapsus$ Hunters”, comprising elements of Scattered Spider, ShinyHunters, and LAPSUS$, accelerating weaponization and widespread exploitation following Oracle’s public disclosure and patch release. CVE-2025-61882 remains a severe enterprise-level threat, enabling unauthenticated attackers to achieve full control of Oracle EBS environments with minimal effort.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-61882	Oracle E-Business Suite versions 12.2.3-12.2.14	cpe:2.3:a:oracle:concurrent_processing:*:*:*:*:*:*:*:*	CWE-22 CWE-444

Recommendations

Patch Immediately : Apply Oracle's Critical Patch Update (CPU) immediately for all affected EBS versions (12.2.3–12.2.14). Verify that patches are fully applied by checking system logs and versioning information.

Restrict Network Exposure: Limit access to Oracle EBS web endpoints (/OA_HTML/SyncServlet, /OA_HTML/RF.jsp, /OA_HTML/OA.jsp) to internal networks or via VPN. Block inbound traffic from untrusted networks and the public internet wherever possible.

Monitor and Detect Exploitation: Implement monitoring for suspicious POST requests targeting the above endpoints. Look for indicators of compromise: unexpected web shells, outbound HTTPS connections to unknown hosts, and anomalous credential usage. Use SIEM or EDR tools to alert on unusual template uploads or BI Publisher activity.

Access Control and Hardening: Review and enforce least-privilege access for EBS users and administrative accounts. Disable any legacy or unnecessary BI Publisher functionality that is exposed to the internet.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0042 Resource Development
TA0005 Defense Evasion	TA0040 Impact	TA0010 Exfiltration	TA0004 Privilege Escalation
TA0006 Credential Access	TA0008 Lateral Movement	TA0011 Command and Control	TA0007 Discovery
T1190 Exploit Public-Facing Application	T1203 Exploitation for Client Execution	T1071.001 Web Protocols	T1071 Application Layer Protocol
T1105 Ingress Tool Transfer	T1059 Command and Scripting Interpreter	T1505.003 Web Shell	T1505 Server Software Component

T1588.006 Vulnerabilities	**T1588.005** Exploits	**T1588** Obtain Capabilities	**T1068** Exploitation for Privilege Escalation
T1078 Valid Accounts	**T1210** Exploitation of Remote Services	**T1041** Exfiltration Over C2 Channel	**T1486** Data Encrypted for Impact

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	200[.]107[.]207[.]26, 185[.]181[.]60[.]11
SHA256	76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d, aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121, 6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b

Patch Details

Prerequisite: The October 2023 Critical Patch Update (CPU) must be applied before installing the CVE-2025-61882 patch.

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

https://www.oracle.com/security-alerts/

https://support.oracle.com/rs?type=doc&id=3106344.1

References

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

https://labs.watchtowr.com/well-well-well-its-another-day-oracle-e-business-suite-pre-auth-rce-chain-cve-2025-61882well-well-well-its-another-day-oracle-e-business-suite-pre-auth-rce-chain-cve-2025-61882/

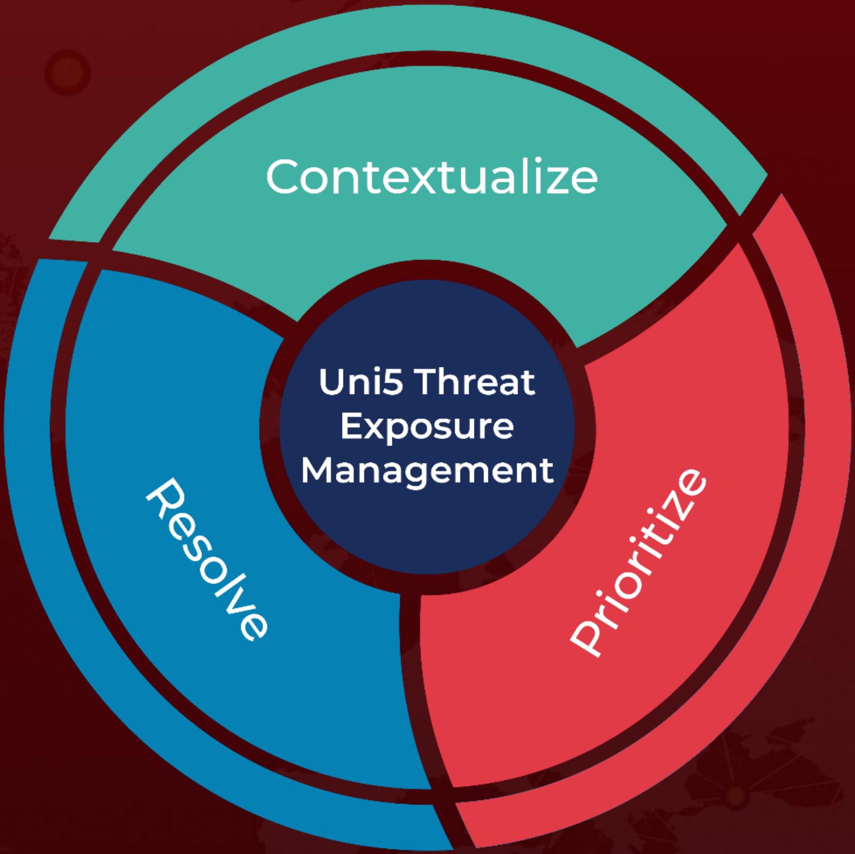
https://www.tenable.com/blog/cve-2025-61882-faq-oracle-e-business-suite-zero-day-cl0p-and-july-2025-cpu

https://x.com/DarkWebInformer/status/1973846461386563641

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 8, 2025 • 6:00 AM

More at www.hivepro.com