American Hospital Association™
Advancing Health in America

Cybersecurity Advisory

October 6, 2025

Hospitals That Are Oracle Customers Urged to Take Immediate Action to Address Security Vulnerability

Oracle has published a Security Alert that addresses vulnerability CVE-2025-61882 in the Oracle E-Business Suite (EBS). This vulnerability is remotely exploitable without authentication, i.e., it may be exploited over a network without the need for a username and password. If successfully exploited, this vulnerability may result in remote code execution. **Oracle strongly recommends that customers apply the updates provided by this Security Alert as soon as possible.**

"This is 'stop-what-you're-doing and patch immediately' vulnerability," Brett Leatherman, FBI Assistant Director, Cyber Division, posted last night on LinkedIn. "The bad guys are likely already exploiting in the wild, and the race is on before others identify and target vulnerable systems."

WHAT YOU CAN DO

- **Please share this Advisory with your cybersecurity and information technology teams and act right away.**
- **Apply Oracle's patch, which is available in the Security Alert. Please note that you must apply the October 2023 Critical Patch Update first — it's a prerequisite.**
- **Isolate or firewall EBS servers so BI Publisher/Concurrent Processing components aren't network-exposed.**
- **Review Oracle's published indicators of compromise and hunt for any signs of compromise.**
- **Monitor your threat intel feeds — exploit activity could escalate quickly.**
- **Contact your local FBI field office if your organization has been compromised by this vulnerability.**

FURTHER QUESTIONS

If you have further questions, please contact John Riggi, AHA national advisor for cybersecurity and risk, at jriggi@aha.org, or Scott Gee, AHA deputy director for cybersecurity and risk, at sgee@aha.org.