4Jawaly Security Advisory - CVE-2026-7632
==========
Generated: 2026-05-02 20:44 UTC
Advisory URL: https://www.4jawaly.com/ar/post/online-hospital-management-system-sql-injection-warning/

CVE ID: CVE-2026-7632
Severity: HIGH
CVSS Score: 7.3
CWE: CWE-74

EXECUTIVE SUMMARY
A vulnerability was determined in code-projects Online Hospital Management System 1.0. This affects an unknown function of the file /viewappointment.php. This manipulation of the argument delid causes sql injection. The attack is possible to be carried out remotely. The exploit has been publicly disclosed and may be utilized.

AFFECTED PRODUCT / COMPONENT
See vendor advisory and affected component details.

RISK FOR HOSTING AND SERVER OPERATORS
This vulnerability may affect websites, hosting panels, plugins, or server-side components. Operators should identify exposed installations, review access controls, inspect logs for suspicious activity, and apply the vendor fix as soon as it becomes available.

RECOMMENDED ACTIONS
1. Update the affected software to the latest patched version. 2. Restrict administrative access and review user privileges. 3. Monitor web server and application logs for exploitation attempts. 4. Apply WAF or virtual patching rules where available. 5. Keep backups and verify recovery procedures.

REFERENCES
- https://code-projects.org/
- https://github.com/Sh1tKing/cve/blob/main/time-blind-sql.md
- https://vuldb.com/submit/806633
- https://vuldb.com/vuln/360578
- https://vuldb.com/vuln/360578/cti

Prepared by 4Jawaly - Security and Web Hosting Alerts