4Jawaly Security Advisory - CVE-2026-2554
==========
Generated: 2026-05-02 20:44 UTC
Advisory URL: https://www.4jawaly.com/ar/post/cve-2026-2554-wcfm-wordpress-idor-user-deletion/

CVE ID: CVE-2026-2554
Severity: HIGH
CVSS Score: 8.1
CWE: CWE-639

EXECUTIVE SUMMARY
The WCFM - Frontend Manager for WooCommerce along with Bookings Subscription Listings Compatible plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 6.7.25 via the 'wcfmdeletewcfmcustomer' due to missing validation on the 'customerid' user controlled key. This makes it possible for authenticated attackers, with Vendor-level access and above, to delete arbitrary users, including Administrators.

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://plugins.trac.wordpress.org/browser/wc-frontend-manager/tags/6.7.24/core/class-wcfm-customer.phpL386
- https://plugins.trac.wordpress.org/changeset/3483695/
- https://www.wordfence.com/threat-intel/vulnerabilities/id/21e397a4-0b32-4b13-a46b-c465acea0796?source=cve

Prepared by 4Jawaly - Security and Web Hosting Alerts