



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Multiple Vulnerabilities in Apache OFBiz
Tracking #:432317999
Date:13-11-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Apache OFBiz, an open-source enterprise resource planning (ERP) platform. These vulnerabilities could allow attackers to gain control of affected systems, execute arbitrary code, or compromise user sessions within enterprise environments.

TECHNICAL DETAILS:

Vulnerability Details

CVE-2025-59118

- Vulnerability Type: Unrestricted Upload of File with Dangerous Type
- Severity: Important
- This flaw allows remote attackers to upload arbitrary files, such as scripts or executables, due to improper validation of file uploads. Exploitation could lead to full system compromise under the privileges of the OFBiz service, enabling attackers to execute arbitrary commands, deploy web shells, or gain persistence.

CVE-2025-61623

- Vulnerability Type: Reflected Cross-Site Scripting (XSS)
- Severity: Important
- This issue enables attackers to inject malicious JavaScript through crafted URLs or input parameters. If exploited, it could result in session hijacking, credential theft, or execution of unauthorized actions within the user's browser, particularly in environments with multiple administrative users.

Affected Versions

- Apache OFBiz versions prior to 24.09.03

Fixed Version

- Apache OFBiz version 24.09.03 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Apache OFBiz.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- <https://www.cve.org/CVERecord?id=CVE-2025-59118>
- <https://www.cve.org/CVERecord?id=CVE-2025-61623>