مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Apache OFBiz

Tracking #:432315928

Date:05-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Critical Vulnerability in Apache OFBiz that could be exploited execute malicious code on vulnerable system.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-36104**
- CVSS v3 Base Score: 9.1 Critical
- A path traversal vulnerability exists in Apache OFBiz that allows an attacker to execute arbitrary code on a vulnerable system. This vulnerability can be exploited remotely by an attacker who can trick a victim into visiting a specially crafted URL.
- The vulnerability exists due to improper validation of user-supplied input within Apache OFBiz. An attacker can exploit this vulnerability by crafting a URL that contains a path traversal payload. When the server processes this URL, it may inadvertently access files outside of its intended directory. This could allow the attacker to execute arbitrary code on the server, potentially taking complete control of the affected system.

Affected Products:

- Apache OFBiz versions before 18.12.14

Fixed Version:

- Apache OFBiz version 18.12.14 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.tenable.com/cve/CVE-2024-36104