مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates – Apache OFBiz

Tracking #:432316538

Date:21-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Apache has released security updates to patch multiple vulnerabilities in the Apache OFBiz.

TECHNICAL DETAILS:

The Apache Software Foundation has released security updates to address two critical vulnerabilities in Apache OFBiz, a widely-used open-source enterprise resource planning (ERP) system. These vulnerabilities could allow remote attackers to execute arbitrary code on vulnerable systems, potentially leading to severe data breaches and system compromises.

Vulnerability Details

- **CVE-2024-47208: Remote Code Execution via Groovy Expression Injection**
  - This vulnerability allows remote attackers to execute arbitrary code on vulnerable systems by exploiting OFBiz's URL handling mechanism. The flaw combines Server-Side Request Forgery (SSRF) and Code Injection vulnerabilities, enabling attackers to inject and execute malicious Groovy expressions.
  - Attackers can gain unauthorized control over the server, potentially compromising sensitive data and business operations.
- **CVE-2024-48962: SameSite Protection Bypass for Cross-Site Attacks**
  - This vulnerability enables attackers to bypass SameSite restrictions, a crucial defense against Cross-Site Request Forgery (CSRF) attacks. The flaw involves a combination of Code Injection, CSRF, and improper neutralization of special elements within OFBiz's template engine.
  - Malicious actors can craft requests that appear to originate from the victim's browser, potentially leading to unauthorized actions and data breaches.

Affected Versions:

- Apache OFBiz versions prior to 18.12.17

Fixed Versions:

- Apache OFBiz version 18.12.17 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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://ofbiz.apache.org/security.html