مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in pac4j Framework

Tracking #:432316396

Date:15-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical vulnerability, identified as CVE-2023-25581, has been discovered in the pac4j-core Java security framework.

TECHNICAL DETAILS:

A critical vulnerability, identified as CVE-2023-25581, has been discovered in the pac4j-core Java security framework, affecting versions prior to 4.0.0. This vulnerability allows attackers to exploit Java deserialization flaws, potentially leading to Remote Code Execution (RCE). The vulnerability arises from inadequate validation of serialized objects stored in user profile attributes, making it possible for malicious actors to inject harmful serialized data.

Vulnerability Details:

- Vulnerability ID: CVE-2023-25581
- CVSS Score: 9.2 (Critical)
- Affected Component: org.pac4j:pac4j-core (versions < 4.0.0)
- Vulnerability Type: Java Deserialization Flaw
- Impact: Potential Remote Code Execution (RCE)
- Affected Versions: All versions of pac4j-core prior to 4.0.0 are vulnerable.

RECOMMENDATIONS:

- Immediate Upgrade: Users of pac4j-core should upgrade to version 4.0.0 or later to eliminate the vulnerability.

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://nvd.nist.gov/vuln/detail/CVE-2023-25581