مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

High Risk Vulnerability in OpenAM

Tracking #:432316109

Date:01-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a Vulnerability in OpenAM that exposes Authentication Systems to Critical Risk and allows remote attackers to execute arbitrary code.

TECHNICAL DETAILS:

CVE-2024-41667 is a severe vulnerability in OpenAM, rated with a **CVSS score of 8.8.** It allows remote attackers to execute arbitrary code through a FreeMarker template injection in the _getCustomLoginUrlTemplate_ method, threatening organizations that utilize OpenAM for authentication, SSO, and authorization.

Vulnerability ID: CVE-2024-41667
Affected Software: OpenAM, part of the Open Identity Platform.
Vulnerability Type: FreeMarker template injection.
Discovery: Reported by researcher AfterSnows, who also provided a proof-of-concept for exploitation.

Mitigations:

- Upgrade: OpenAM version 15.0.4 or later
- Implement Security Measures: Utilize _TemplateClassResolver.SAFER_RESOLVER_ to restrict class resolution in FreeMarker templates.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the OpenAM to the fixed version.

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://github.com/OpenIdentityPlatform/OpenAM/security/advisories/GHSA-7726-43hg-m23v