مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Keycloak Unauthorized Access Vulnerability

Tracking #:432316397

Date:16-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability has been identified in Keycloak, allowing low-privileged users to access administrative functionalities within the Keycloak admin interface.

TECHNICAL DETAILS:

A high severity vulnerability has been identified in Keycloak versions prior to 24.0.5, allowing low-privileged users to access administrative functionalities within the Keycloak admin interface. This flaw poses a significant security risk, potentially leading to unauthorized actions that could compromise sensitive data and system integrity. Organizations using affected versions are urged to take immediate action to mitigate risks associated with this vulnerability.

Vulnerability Details:

- **CVE Identifier**: CVE-2024-3656
- **Severity**: High (CVSS Score: 8.1)
- **Affected Versions**: Keycloak versions < 24.0.5
- **Patched Version**: 24.0.5

RECOMMENDATIONS:

- Upgrade Keycloak version to fixed version or later to patch 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://github.com/advisories/GHSA-2cww-fgmg-4jqc