مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Update - Keycloak

Tracking #:432317488

Date:15-07-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a moderate severity vulnerability was disclosed in Keycloak's account merging process during identity provider (IdP) login. This flaw allows attackers to impersonate victims by exploiting email verification during login.

TECHNICAL DETAILS:

An authenticated attacker can exploit Keycloak's "Review Profile" step during IdP login to change their email address to match a victim's. This triggers a verification email to the victim without showing the attacker's email, creating a phishing opportunity. If the victim clicks the link, the attacker gains access to the victim's account

Vulnerability Details:

- **CVE ID**: CVE-2025-7365
- **Package**: org.keycloak:keycloak-services (Maven)
- **Affected Versions**: < 26.3.0
- **Fixed Version**: 26.3.0
- **Severity**: 5.4 Moderate

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the latest updates released by Keycloak 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://github.com/advisories/GHSA-gj52-35xm-gxjh