



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



High Severity Vulnerability in Keycloak

Tracking #:432316313

Date:23-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability, tracked as CVE-2024-8698, has been identified in Keycloak's SAML signature validation process.

TECHNICAL DETAILS:

A high-severity vulnerability, tracked as CVE-2024-8698, has been identified in Keycloak's SAML signature validation process. This flaw allows attackers to bypass authentication mechanisms, potentially leading to privilege escalation and impersonation attacks.

Vulnerability Details:

- **CVE Identifier:** CVE-2024-8698
- **CVSS Score:** 7.7 (High)
- **Description:** The class incorrectly determines whether a signature applies to the entire SAML document or specific assertions, allowing attackers to craft malicious SAML responses that can bypass authentication.

Affected Versions:

- Keycloak versions up to and including 25.0.5

Fixed Version:

- Keycloak versions 25.0.6

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://nvd.nist.gov/vuln/detail/CVE-2024-8698>