مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates - Keycloak

Tracking #:432316562

Date:27-11-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Keycloak has released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Keycloak, an open-source identity and access management platform, has released security updates to address multiple vulnerabilities. These vulnerabilities pose various risks, including denial-of-service (DoS) attacks, information disclosure, and authentication bypass.

Vulnerabilities Details:

- **CVE-2024-10039 (CVSS 7.1):** In deployments using mutual TLS (mTLS) authentication, an attacker on the local network could bypass authentication and impersonate users or clients. This affects deployments with a reverse proxy not using pass-through termination of TLS, with mTLS enabled
- **CVE-2024-10270 (CVSS 6.5):** A vulnerability in the SearchQueryUtils method could allow attackers to trigger a DoS attack by exhausting system resources.
- **CVE-2024-10451 (CVSS 5.9):** Sensitive information, such as passwords, could be embedded in bytecode during the build process, leading to potential information disclosure
- **CVE-2024-10492 (CVSS 2.7):** Allows a high-privileged user to potentially access sensitive information from a Vault file
- **CVE-2024-9666 (CVSS 4.7):** A DoS vulnerability related to improper handling of proxy headers

Affected Versions

- Keycloak versions prior to 24.0.9
- Keycloak versions prior to 26.0.6

Fixed Versions:

- Keycloak 24.0.9
- Keycloak 26.0.6

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://github.com/keycloak/keycloak/security/advisories/