مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Apache HttpClient

Tracking #:432318847

Date:27-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a High-Severity vulnerability in Apache HttpClient allows an attacker to bypass SCRAM-SHA-256 mutual authentication, potentially leading to unauthorized access in client-server communications.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE ID:** CVE-2026-40542
- **Severity:** High
- Apache HttpClient contains a missing critical step in the SCRAM-SHA-256 mutual authentication process. This flaw may allow an attacker to manipulate the authentication flow, causing the client to incorrectly accept authentication without proper verification. As a result, an attacker could bypass authentication controls and establish unauthorized trusted sessions.

Affected Products

- Apache HttpClient 5.6

Fixed Versions

- Apache HttpClient 5.6.1 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Apache.

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-2026-40542