مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerability in Apache Log4j Core

Tracking #:432318167

Date:23-12-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a vulnerability in Apache Log4j Core's Socket Appender that could allow attackers to intercept or redirect sensitive log data due to missing TLS hostname verification.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2025-68161**
- **CVSS Score:** 6.3 (Medium)
- **Vulnerability Type:** Missing TLS Hostname Verification
- **Affected Component:** Apache Log4j Core (Socket Appender)
- The vulnerability resides in the *Socket Appender* component, which is responsible for transmitting log data over the network to a remote logging server. Affected versions fail to properly verify the hostname in the server's TLS certificate during secure connections.
- Even when hostname verification is explicitly enabled through configuration settings or system properties, the affected Log4j versions do not enforce this validation. As a result, the application may establish a trusted connection with an unintended or malicious server.

Impact

This flaw enables **Man-in-the-Middle (MitM)** attacks, allowing attackers positioned between the application and the log server to intercept or redirect log traffic. Because application logs often contain sensitive operational details, credentials, or user-related information, successful exploitation could lead to information disclosure and facilitate further attacks within the environment.

Affected Versions

- Apache Log4j Core (org.apache.logging.log4j:log4j-core) 2.0-beta9 before 2.25.3

Fixed Version

- Apache Log4j Core 2.25.3 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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-2025-68161