مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Apache Uniffle
Tracking #:432318234
Date:12-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Apache Uniffle that could allow man-in-the-middle (MITM) attacks due to insecure default SSL/TLS settings in the HTTP client.

TECHNICAL DETAILS:

A critical vulnerability has been identified in Apache Uniffle. Tracked as CVE-2025-68637 with a CVSS score of 9.1 (Critical), the flaw exposes Uniffle deployments to Man-in-the-Middle (MITM) attacks due to insecure default SSL/TLS settings in the Uniffle HTTP client.

Vulnerability Details
- **CVE-2025-68637**
- **Severity:** Critical
- **CVSS v3 Score:** 9.1
- The vulnerability arises from how the Apache Uniffle HTTP client establishes SSL/TLS connections. By default, the client is configured to trust all SSL/TLS certificates and to disable hostname verification. This effectively nullifies core TLS security guarantees. An attacker with network access could impersonate the Uniffle Coordinator service by presenting a forged certificate, allowing them to intercept or manipulate REST API communications between the Uniffle client/CLI and the Coordinator without detection.
- Successful exploitation could allow a network-based attacker to perform MITM attacks, leading to unauthorized interception or manipulation of control traffic and potentially sensitive data within distributed computing pipelines.

Affected Versions
- Apache Uniffle versions prior to 0.10.0

Fixed Versions
- Apache Uniffle 0.10.0 and 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://www.tenable.com/cve/CVE-2025-68637