مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Apache Storm

Tracking #:432318774

Date:13-04-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Apache Storm; these vulnerabilities could allow authenticated attackers to execute arbitrary code or compromise administrator sessions.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-35337**
  - **Severity:** Important
  - The Storm Client improperly deserializes a base64-encoded Kerberos TGT using ObjectInputStream.readObject() without validation. An authenticated attacker can submit a crafted object via the Nimbus Thrift API, resulting in remote code execution (RCE) on Nimbus and Worker nodes.

- **CVE-2026-35565**
  - **Severity:** Moderate
  - The Storm UI inserts topology metadata directly into HTML using innerHTML without sanitization. An authenticated attacker can inject JavaScript, leading to stored XSS when an administrator views the topology, potentially enabling session hijacking or privilege abuse.

Affected Versions

- Apache Storm < 2.8.6

Fixed Version

- Apache Storm 2.8.6 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Apache Storm.

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://lists.apache.org/thread/tsv264jx9mo3qm44snpogtono9zm128l
- https://lists.apache.org/thread/98b9fp9t77y2m4m3l1msxkjz59tqlpvg