مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

RCE Vulnerabilities in Kafka UI

Tracking #:432315979

Date:25-06-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Kafka released security updates to address security flaws impacting its UI that allows remote code execution by an unauthenticated attacker.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-32030**
  - **CVSS Score: 8.1 – High**
  - An attacker can exploit this feature by connecting Kafka UI to a malicious JMX server and by returning a malicious serialized object, the attacker can achieve RCE.
  - **Prerequisites**: Either *dynamic.config.enabled* is set or the attacker has access to the Kafka cluster connected to Kafka UI.

- **CVE-2023-52251**
  - **CVSS Score: 8.8 – High**
  - Kafka UI allows users to display messages from Kafka clusters based on user-provided filters. An attacker can abuse this filter to execute arbitrary code on the server. Kafka UI does not have authentication enabled by default, making this vulnerability particularly dangerous.

Affected Versions:

- Kafka UI versions 0.4.0 through 0.7.1.

Fixed Versions:

- Kafka UI version 0.7.2 and later releases.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update the affected versions to the fixed version released by Kafka.

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://securitylab.github.com/advisories/GHSL-2023-229_GHSL-2023-230_kafka-ui/#/