مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Kibana

Tracking #:432316785

Date:24-01-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Kibana, an open-source data visualization and exploration tool. These vulnerabilities could potentially allow unauthorized access to sensitive information and enable attackers to conduct server-side request forgery attacks.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2024-43707 (High Severity)**:
  - CVSSv3.1 score 7.7
  - This flaw allows unauthorized users to access sensitive information in Elastic Agent policies. The nature of the sensitive information varies based on the integrations and configurations enabled.
  - **Affected Versions**: Kibana versions from 8.0.0 up to 8.15.0
- **CVE-2024-43710 (Medium Severity)**:
  - CVSSv3.1 score 4.3
  - A server-side request forgery (SSRF) vulnerability in the /api/fleet/health_check API, enabling attackers to send unauthorized requests to internal endpoints.
  - **Affected Versions**: Kibana versions from 8.7.0 up to 8.15.0.

Fixed Versions:

- Kibana version **8.15.0** or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-2024-43707
- https://nvd.nist.gov/vuln/detail/CVE-2024-43710