مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Kibana

Tracking #:432317226

Date:07-05-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Kibana that could be exploited to execute malicious commands on vulnerable Kibana deployments.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2025-25014**
- CVSS Score: 9.1 Critical
- A prototype pollution vulnerability exists in Kibana. This flaw allows remote attackers to execute arbitrary code on affected Kibana instances by sending specially crafted HTTP requests to the Machine Learning and Reporting endpoints. Both self-hosted and Elastic Cloud deployments are affected if these features are enabled.
- Successful exploitation allows unauthenticated attackers to manipulate JavaScript object prototypes, potentially overriding application logic and escalating to remote code execution. This poses a severe risk to environments that process sensitive telemetry and analytics data.

Affected Versions

- Kibana 8.3.0 – 8.17.5
- Kibana 8.18.0
- Kibana 9.0.0

Fixed versions:

- Kibana Versions 8.17.6, 8.18.1, or 9.0.1

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Kibana.

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-2025-25014