مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Multiple Vulnerabilities in Elastic Kibana

Tracking #:432318007

Date:14-11-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Elastic Kibana, the visualization and analytics dashboard component of the Elastic Stack. The flaws could allow attackers to perform Server-Side Request Forgery (SSRF) and DOM-based Cross-Site Scripting (XSS) attacks.

TECHNICAL DETAILS:

Elastic has disclosed two vulnerabilities in Kibana, the analytics dashboard for the Elastic Stack, that could enable Server-Side Request Forgery (SSRF) and DOM-based Cross-Site Scripting (XSS) attacks. The flaws — CVE-2025-37734 (CVSS 4.3) and CVE-2025-59840 (CVSS 8.7) — affect multiple Kibana versions across Elastic Cloud and self-hosted deployments.

Vulnerability Details

CVE-2025-59840 – Improper Input Sanitization / DOM-based Cross-Site Scripting (XSS)

- **CVSS Score:** 8.7 (High)
- An improper input sanitization vulnerability in Kibana's Vega visualization engine could allow attackers to inject and execute arbitrary JavaScript in the victim's browser.
- Successful exploitation could result in session hijacking, data theft, or execution of malicious scripts within the user's Kibana session.

CVE-2025-37734 – Origin Validation Error / Server-Side Request Forgery (SSRF)

- **CVSS Score:** 4.3 (Medium)
- A flaw in the Origin validation logic within Kibana's Observability AI Assistant can be exploited to perform Server-Side Request Forgery (SSRF) attacks.
- Attackers could send malicious HTTP requests with forged Origin headers, tricking Kibana into making requests to internal systems, potentially exposing sensitive data or enabling further compromise.

Affected Versions

These vulnerabilities impact multiple versions of Kibana prior to:

- 8.19.7
- 9.1.7
- 9.2.1

Fixed Versions

- Kibana 8.19.7
- Kibana 9.1.7
- Kibana 9.2.1

RECOMMENDATIONS:

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

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://discuss.elastic.co/t/kibana-8-19-7-9-1-7-9-2-1-security-update-esa-2025-25/383379
- https://discuss.elastic.co/t/kibana-8-19-7-9-1-7-and-9-2-1-security-update-esa-2025-24/383381