مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerability in Kibana

Tracking #:432317417

Date:26-06-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Elastic has released security updates for multiple Kibana versions to address a critical vulnerability.

TECHNICAL DETAILS:

Elastic has released security updates for multiple Kibana versions to address a critical vulnerability (CVE-2025-2135), which originates from a Chromium Type Confusion flaw that may lead to heap corruption when processing crafted HTML pages. This issue impacts both self-hosted and Elastic Cloud Kibana instances where PDF or PNG reporting is enabled. The vulnerability could allow remote attackers to execute arbitrary code within the reporting environment, posing a significant risk to organizations using affected Kibana versions.

Technical Details

- **CVE ID:** CVE-2025-2135
- **Vulnerability Type:** Heap corruption via Chromium Type Confusion
- **Impact:** Remote Code Execution in the Kibana reporting environment
- **Attack Vector:** Network
- **Privileges Required:** Low
- **User Interaction:** None
- **Exploitability:** High
- **Severity: Critical**

Impacted Versions
The vulnerability affects Kibana installations in the following version ranges:

- 7.x: Up to and including 7.17.28
- 8.x: From 8.0.0 up to and including 8.17.7, and 8.18.0 up to and including 8.18.2
- 9.x: From 9.0.0 up to and including 9.0.2

Only deployments using PDF or PNG reporting are affected. CSV reporting and serverless Kibana projects are not impacted.

Fixed Versions

- 7.17.29
- 8.17.8
- 8.18.3
- 9.0.3

RECOMMENDATIONS:

- Upgrade Immediately: All users are strongly advised to upgrade to the latest patched versions.
- Organizations unable to patch immediately should apply the provided mitigations to reduce risk exposure.

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-7-17-29-8-17-8-8-18-3-9-0-3-security-update-esa-2025-09/379443/1