CERT-EU

Security Advisory 2025-007

Critical Vulnerability in Kibana

2025-03-06 — v1.0

TLP:CLEAR

History:

- *06/03/2025 — v1.0 – Initial publication*

Summary

On 5 March 2025, Elastic released a security update addressing a critical vulnerability in Kibana, identified as **CVE-2025-25012** with a CVSS score of 9.9 [1].

This flaw could allow an attacker to execute arbitrary code on the server. It is strongly recommended to update vulnerable Kibana instances.

Technical Details

The vulnerability **CVE-2025-25012** arises from prototype pollution in Kibana, leading to arbitrary code execution via a crafted file upload and specifically crafted HTTP request [1].

Products Affected

In Kibana versions >= 8.15.0 and < 8.17.1, the vulnerability is exploitable by users with the Viewer role. In Kibana versions 8.17.1 and 8.17.2, this is only exploitable by users that have roles that contain all the following privileges: `fleet-all`, `integrations-all`, `actions:execute-advanced-connectors` [1].

Recommendations

CERT-EU recommends updating to Kibana version 8.17.3 as soon as possible.

Mitigations

For users who cannot upgrade immediately, Elastic advises to set the `xpack.integration_assistant.enabled` configuration option to `false` in Kibana's configuration (`kibana.yml`) [1].

References

[1] https://discuss.elastic.co/t/kibana-8-17-3-security-update-esa-2025-06/375441