CVE-2025-2135: KIBANA HEAP CORRUPTION VIA CRAFTED HTML PAGE

Vairav CVE Report

Date: June 26, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Elastic has disclosed critical vulnerability (CVE-2025-2135) in Kibana's PDF/PNG reporting feature, caused by a Chromium Type Confusion flaw. This issue may lead to heap corruption and potential remote code execution in affected self-hosted and Elastic Cloud instances. Kibana versions up to 9.0.2 are impacted, and immediate updates or mitigations are recommended.

VULNERABILITY DETAILS

CVE-2025-2135: Kibana Heap Corruption via Crafted HTML Page

Description: A Type Confusion vulnerability in Chromium (CVE-2025-2135) used by Kibana's reporting engine can lead to heap corruption via crafted HTML input. Exploitation allows remote code execution within the Kibana service if PDF/PNG report generation is enabled.

Impact: Remote Code Execution (RCE)

CVSS Score: 9.9 (Critical)

AFFECTED PRODUCTS/VERSIONS

- Kibana 7.0.0 – 7.17.28
- Kibana 8.0.0 – 8.17.7
- Kibana 8.18.0 – 8.18.2
- Kibana 9.0.0 – 9.0.2

Note: *Only affects instances with PDF/PNG Reporting enabled. CSV reporting and serverless deployments are not impacted.*

EXPLOIT DETAILS

An attacker can exploit vulnerability by submitting or triggering malicious HTML content in a report request, leveraging Chromium's type confusion flaw. This causes heap corruption, potentially leading to code execution within the reporting container.

RECOMMENDED ACTIONS

For Self-hosted Kibana:

- **Upgrade to** 7.17.29, 8.17.8, 8.18.3, or 9.0.3.

- **If unable to upgrade:**
  - Disable Reporting:

```
xpack.reporting.enabled: false
```

  - Limit reporting access to trusted users (see Elastic documentation for versions 8.x and 9.x)
  - Implement restrictive network policies:

```
xpack.screenshotting.networkPolicy:
  rules: [ { allow: true, host: "localhost:5601" } ]
```

For Elastic Cloud Users:

- Risk is reduced due to container isolation (AppArmor, seccomp-bpf)
- Additional steps if an upgrade is not possible:
  - Disable reporting via Kibana user settings:

```
xpack.reporting.enabled: false
```

  - Restrict access to PDF/PNG reporting to trusted users.

REFERENCES

https://securityonline.info/critical-kibana-flaws-cve-2025-2135-cvss-9-9-allows-heap-corruption-open-redirect-also-patched/

http://discuss.elastic.co/t/kibana-7-17-29-8-17-8-8-18-3-9-0-3-security-update-esa-2025-09/379443

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com