CVE-2025-25012: KIBANA ARBITRARY CODE EXECUTION VIA PROTOTYPE POLLUTION

Vairav CVE Report

Date: March 06, 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 a critical security vulnerability (CVE-2025-25012) in Kibana that allows arbitrary code execution via prototype pollution. This flaw affects Kibana versions 8.15.0 through 8.17.2. Exploiting this vulnerability requires an attacker to upload a specially crafted file and send specific HTTP requests. The risk varies based on user roles, with broader exposure in versions before 8.17.1. Organizations using affected versions should immediately apply mitigation measures or upgrade to Kibana 8.17.3.

VULNERABILITY DETAILS

CVE-2025-25012: Kibana Arbitrary Code Execution via Prototype Pollution

Description: This vulnerability enables attackers to execute arbitrary code through prototype pollution. Affected versions allow exploitation via crafted file uploads and specially constructed HTTP requests.

Impact: Unauthorized system control, data compromise, and potential lateral movement within affected environments.

CVSS Score: 9.9 (Critical)

AFFECTED VERSIONS

- Kibana versions 8.15.0 - 8.17.2

EXPLOIT DETAILS

- **Pre 8.17.1:** Exploitable by users with the Viewer role.
- **8.17.1 and 8.17.2:** Requires roles containing the following privileges: fleet-all, integrations-all, and actions:execute-advanced-connectors.
- Attackers can craft malicious payloads that manipulate object prototypes, leading to unauthorized command execution.

RECOMMENDED ACTIONS

- Upgrade to Kibana 8.17.3 immediately to mitigate this vulnerability.

For Users Unable to Upgrade:

- Set xpack.integration_assistant.enabled: false in Kibana’s configuration file to disable vulnerable functionality.

ADDITIONAL SECURITY MEASURES

- Restrict access to Kibana interfaces to only trusted users.
- Enable enhanced logging to detect unauthorized attempts to exploit prototype pollution vulnerabilities.
- Conduct periodic reviews of role-based access controls and Kibana configurations.

REFERENCES

https://securityonline.info/cve-2025-25012-cvss-9-9-critical-code-execution-vulnerability-patched-in-elastic-kibana/

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

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