BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2025-36
Fecha de publicación: 7/05/2025
Tema: Vulnerabilidad RCE en Kibana
Traffic Light Protocol (TLP): White

Producto(s) afectado(s):

La vulnerabilidad afecta a las versiones de Kibana:

- 8.3.0 a 8.17.5
- 8.18.0
- 9.0.0

Descripción

Se ha reportado una nueva vulnerabilidad crítica en Kibana de Elastic, la misma fue identificada como CVE-2025-25014, con una puntuación CVSS de 9.1. Esta falla se deriva de una vulnerabilidad de contaminación de prototipos (Prototype Pollution DOM) que puede provocar la ejecución de código arbitrario mediante solicitudes HTTP especialmente diseñadas dirigidas a los endpoints de aprendizaje automático e informes de Kibana.

Las vulnerabilidades de contaminación de prototipos (Prototype Pollution) manipulan el prototipo del objeto (DOM) en el JavaScript subyacente, lo que permite a los atacantes inyectar propiedades maliciosas que pueden anular la lógica de la aplicación. En este caso, la vulnerabilidad escala a la ejecución remota de código, el peor escenario posible para entornos de monitoreo que suelen gestionar telemetría y análisis sensibles.

Tanto las implementaciones autohospedadas como las de Elastic Cloud son vulnerables si tienen habilitadas las funciones de aprendizaje automático e informes.

Mitigación

Para los usuarios que no pueden actualizar, Elastic ofrece dos rutas de mitigación:

1. Deshabilitar el aprendizaje automático
    - Agregue lo siguiente a **kibana.yml**:

```
xpack.ml.enabled: false
```

    - Alternativamente, para deshabilitar solo la detección de anomalías:

```
xpack.ml.ad.enabled: false
```

2. Ó, Deshabilitar informes
    - Agregue lo siguiente a **kibana.yml**:

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

Solución

El equipo de Elastic recomienda aplicar actualizar inmediatamente a las siguiente versiones corregidas:

- 8.17.6
- 8.18.1
- 9.0.1

Para encontrar información sobre el proceso de actualización dirijase al siguiente enlace: https://www.elastic.co/docs/deploy-manage/upgrade/deployment-or-cluster

Información adicional:

- https://discuss.elastic.co/t/kibana-8-17-6-8-18-1-or-9-0-1-security-update-esa-2025-07/377868
- https://securityonline.info/cve-2025-25014-cvss-9-1-prototype-pollution-in-kibana-opens-door-to-code-execution/

BEACON LAB

C S I R T

CYBOLT

Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com