BEACON LAB
C S I R T

CYBOLT
Security Innovation

Boletín de Alerta

Boletín Nro.: 2024-29
Fecha de publicación: 10/09/2024
Tema: Vulnerabilidad crítica en Kibana
Traffic Light Protocol (TLP): White

Producto(s) afectado:

- Kibana versiones 8.15.1 y anteriores.

Descripción

El equipo de Elastic publicó dos vulnerabilidades críticas, identificadas como CVE-2024-37288 y CVE-2024-37285 con score CVSS de 9.9 y 9.3 respectivamente, las cuales afectan la versión 8.15.1 y anteriores de Kibana, ambas vulnerabilidades permiten la ejecución de código arbitrario (RCE).

A continuación se listan ambas vulnerabilidades y sus detalles relevantes:

CVE-2024-37288: con un score de CVSSv3 de 9.9, es un problema de deserialización en Kibana que puede provocar la ejecución de código arbitrario (RCE) intenta analizar un documento YAML que contiene un payload manipulado. Este problema solo afecta a los usuarios que utilizan las herramientas de IA integradas de Elastic Security y han configurado un conector de Amazon Bedrock.

CVE-2024-37285: Con un score CVSSv3 de 9.1, también relacionada con la deserialización de YAML, afecta a un rango más amplio de usuarios de Kibana. Permite a los atacantes ejecutar código arbitrario (RCE) si poseen privilegios específicos de índices de Elasticsearch y privilegios de Kibana. El atacante necesita acceso de escritura a los índices del istema (.kibana_ingest) * y la capacidad de administrar índices restringidos. También debe tener ciertos privilegios de Kibana en Fleet (All) e Integration (Read o All), y obtener acceso al privilegio de configuración de Fleet a través del token de cuenta de servicio de Fleet Server.

Solución

Para solucionar ambas vulnerabilidades se recomienda actualizar a la versión 8.15.1, puede encontrar la actualización en el siguiente enlance:
https://discuss.elastic.co/t/kibana-8-15-1-security-update-esa-2024-27-esa-2024-28/366119

Se recomienda actualizar de inmediato.

Mitigación

En caso que no pueda realizar una actualización por problemas de compatiblidad puede realizar una mitigación temporal para CVE-2024-37288 (esta mitigación no protege contra la vulnerabilidad CVE-2024-37285), para ello debe deshabilitar el asistente de integración:

```
xpack.integration_assistant.enabled: false
```

- https://cybersecuritynews.com/kibana-vulnerabilities/
  https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2024-37288

BEACON LAB
C S I R T

CYBOLT
Security Innovation

info@beaconlab.mx

beaconlab.mx

contact@cybolt.com

cybolt.com