Open Elasticsearch

1. INTRODUCCIÓN

Elasticsearch es un almacén de datos que permite indexar una gran volumen de datos y posteriormente hacer consultas sobre ellos, esta basado en Lucene para indexar y buscar datos. Elasticsearch expone su funcionalidad a través de una interfaz REST recibiendo y enviando datos en formato JSON y oculta mediante esta interfaz los detalles internos de lucene. Esta interfaz permite que pueda ser utilizada por cualquier plataforma no solo Java, puede usarse desde Python, .NET, PHP o incluso desde un navegador con Javascript. Elasticsearch está desarrollado en Java y está publicado como código abierto bajo las condiciones de la licencia Apache.

Elasticsearch usa sus propios conceptos y aunque no es una base de datos relacional puede ser similar, con las bases de datos relacionales existe el concepto de control de acceso donde se puede bloquear el acceso a ciertas bases de datos, columnas o tablas, basadas en usuarios o grupos. Elasticsearch no tiene tal concepto o un control de acceso.

2. RIESGO

De forma predeterminada, este servicio no admite la autenticación, no restringe el acceso al lugar donde se almacenan los datos lo que significa que cualquier entidad que puede acceder a la instancia de Elasticsearch puede tener acceso sin restricciones al almacén de datos y así tener control total del servidor.

Elasticsearch es una herramienta potente no sólo para los desarrolladores, sino también para los administradores de sistemas. Algunas personas registran casi todo en Elasticsearch, incluyendo datos confidenciales. Por lo tanto, es muy importante que restrinja quién puede acceder a los clústeres de Elasticsearch, así como lo que está registrando en ellos.

Si está utilizando Elasticsearch en un entorno de desarrollador y se puede confiar en las demás personas de la red, es probable que no preocupe la seguridad, siempre y cuando no se almacene nada sensible en Elasticsearch. Sin embargo, si se desea exponer un clúster Elasticsearch a la Internet pública, debe bloquearse accesos, así como realizar pruebas periódicas de seguridad.

Por ejemplo, con una aplicación PHP que usa Elasticsearch para almacenar datos de todos sus diferentes clientes, y si uno de esos clientes encuentra un error en la aplicación que le diera acceso directo a Elasticsearch, podría acceder a los datos de todos los índices y acceder a los datos que pertenecen a otros clientes. Si la aplicación utilizando una base de datos relacional como MySQL o Postgresql, se puede bloquear el acceso dándole a cada cliente acceso sólo a determinadas columnas y tablas en una base de datos, el complemento comercial Elasticsearch, SHIELD, soluciona este problema.

Lucene, a su vez, almacena los datos en disco en su propio formato que no está cifrado. Un atacante que obtiene acceso no autorizado a los nodos Elasticsearch puede robar el almacén de datos de Lucene.

3. DETECCIÓN

Los reportes realizados identifican a los host que cuentan con Elasticsearch y son accesibles desde internet.

El comando que permite esta verificación es:

"curl -XGET http: // [ip]: 9200 /"

Si Elasticsearch se está ejecutando, se verá información sobre el servidor Elasticsearch en la pantalla.

INFORMACIÓN DE LOS CAMPOS DEL REPORTE

Campo	Descripción
Vulnerabilidad	Hace referencia al nombre de la vulnerabilidad
Dirección IP	Dirección IP del dispositivo en cuestión
Puerto	Puerto que responde a la vulnerabilidad
timestamp_EcuCERT	Fecha y hora de comprobación de EcuCERT en GMT -5
as_name	Nombre del ASN al que pertenece la dirección IP
status_EcuCERT	Online: vulnerabilidad reportada por *Stakeholders* y comprobada por el EcuCERT en el timestamp_EcuCERT Offline: Vulnerabilidad reportada por *Stakeholders*, pero en el timestamp_EcuCERT no se detectó.
timestamp	Fecha y hora de comprobación en UTC+0
ip	Dirección IP del host
protocol	Protocolo por el que ingresó la respuesta (UDP)
port	Puerto desde donde se obtiene la respuesta Chargen
hostname	DNS reverso del host
tag	Siempre será chargen
version	Número de versión del elasticsearch
asn	ASN de la red donde se encuentra el host
geo	País donde se encuentra el host
region	Estado/Provincia/Región donde se encuentra el host
city	Ciudad donde se encuentra el host
naics	Código del Sistema de Clasificación Industrial de América del Norte
sic	Código del Sistema de Clasificación Industrial Estándar
ok	Indica que todo está funcionando apropiadamente
name	Nombre de identificación de la instancia de Elasticsearch
cluster_name	Nombre de cluster de Elasticsearch a la que pertenece la instancia (si tiene)
status	Usualmente "200", significa que todo está trabajando

Campo	Descripción
build_hash	Hash de la versión de Elasticsearch que está corriendo
build_timestamp	Fecha y hora de cuando fue construida la versión de Elasticsearch que está corriendo
build_snapshot	Si los snapshots está habilitados
lucene_version	Versión del Apache Lucene que Elasticsearch está usando

4. ACCIONES RECOMENDADAS

Para evitar esta vulnerabilidad se recomienda tomar las siguientes medidas:

1. Elasticsearch debe estar detrás de un firewall.
2. Se debe bloquear el puerto 9200, así como el puerto 9300.
3. No correr Elasticsearch como “root”.
4. Agregar autenticación a Elasticsearch

5. REFERENCIAS

- https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-Elasticsearch
- http://www.adictosaltrabajo.com/tutoriales/primeros-pasos-elasticsearch/
- https://www.elastic.co/blog/found-elasticsearch-security#staying-safe-while-developing-with-elasticsearch
- http://blog.shadowserver.org/2014/03/28/the-scannings-will-continue-until-the-internet-improves/
- https://qbox.io/blog/how-to-lock-down-elasticsearch-kibana-logstash-maintain-security
- https://www.ibm.com/support/knowledgecenter/en/SS6PEW_9.5.0/com.ibm.help.security.plan.doc/security/c_SecuringElasticsearchServers.html
- https://support.alertlogic.com/hc/en-us/articles/115002827406-Mitigating-Risks-of-Elasticsearch-Deployment-Best-Practices
- https://picodotdev.github.io/blog-bitix/2014/04/introduccion-a-elasticsearch/