
	SEGURIDAD DE LA INFORMACIÓN	
	VULNERABILIDAD MongoDB	



La información podrá ser compartida libremente de acuerdo con las reglas y procedimientos aplicables para la divulgación pública debe regirse a las normas estándar de derechos de autor.

Vulnerabilidad MongoDB

1. INTRODUCCIÓN

MongoDB es un sistema de base de datos de código abierto orientado a documentos. Se basa en colecciones de documentos Json¹, lo que le otorga una gran flexibilidad en cuanto a la naturaleza de la información que almacena, puesto que puede haber documentos con diferente esquema dentro de una misma colección.

De MongoDB se destaca su gran velocidad y escalabilidad, porque puede manejar sin esfuerzo volúmenes de datos del orden de gigabytes.

2. RIESGO

MongoDB cuenta con productos de pago y otros gratuitos. Son estos últimos los que carecen de seguridad por defecto y, por lo tanto, están expuestos a los ataques, los mismos que pueden ser evitados una vez que se implementen las seguridades adecuadas.

El riesgo radica en caso de que no se cuente con seguridades o estén mal configuradas, toda la información almacenada mediante la base de datos MongoDB puede ser reemplazada, borrada, alterada. Debido a una incorrecta configuración de estas opciones de seguridad, estas bases de datos aceptan conexiones desde fuera de la red local a través del puerto 27017.



En algunos casos, cuando la vulnerabilidad MongoDB es explotada por ciberdelinquentes, la información puede ser secuestrada hasta que el dueño de la información otorgue una cantidad económico para la entrega de la misma.

3. DETECCIÓN

Para la detección de esta vulnerabilidad se usa el comando:



```
nmap -p27017 [ip]
```

¹ JSON (JavaScript Object Notation).- es un formato para el intercambio de datos

	SEGURIDAD DE LA INFORMACIÓN	
	VULNERABILIDAD MongoDB	

INFORMACIÓN DE LOS CAMPOS ADJUNTOS AL REPORTE:

Campo	Descripción
vulnerabilidad	Nombre de la vulnerabilidad reportada
direccion_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
status_EcuCERT	Estado de la vulnerabilidad Online: vulnerabilidad reportada por Feeds y comprobada por el EcuCERT en el timestamp_EcuCERT Offline: Vulnerabilidad reportada por Feeds, pero en el timestamp_EcuCERT no se detectó.
timestamp	Tiempo en la que la IP fue probada en UTC+0
ip	Dirección IP del dispositivo en cuestión
port	Puerto que la respuesta NTP vino
hostname	Nombre DNS inversa del dispositivo en cuestión
tag	Siempre será mongodb
Version	Número del versión de mongodb
asn	ASN en donde el dispositivo en cuestión se aloja
geo	País en donde el dispositivo en cuestión reside
region	Provincia
naics	Código del sistema de clasificación industrial de América del norte
sic	Código del sistema de clasificación industrial estándar
gitversion	Parte del Dominio/IP de la URL
sysinfo	Version de OpenSSL en uso
allocator	Memory allocator en uso
Javascriptengine	Motor del JavaScript usado por MongoDB
server	Software del lado del servidor como Apache / Nginx
Bits	Arquitectura del procesador
Maxbsonobjectsize	Tamaño de documento máximo BSON
Visible_databases	Una lista de 5 bases de datos que corre sobre una instancia de MongoDB. Si la autenticación está en uso, o por alguna razón las bases de datos no se pueden obtener este será asignado como "none visible"

	SEGURIDAD DE LA INFORMACIÓN	
	VULNERABILIDAD MongoDB	

4. ACCIONES RECOMENDADAS

- Verificar que las configuraciones de seguridad de la base de datos de MongoDB se encuentren realizadas correctamente.
- Configurar correctamente los sistemas de inicio de sesión para que no puedan acceder por completo a las bases de datos sin mayor dificultad.
- Realizar copias continuas de las bases de datos.
- Los administradores que quieren evitar que su base de datos sea tomada deben actualizar a la última versión.

5. REFERENCIAS

- <https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-MongoDB>
- <http://blog.hostdime.com.co/vulnerabilidad-en-gui-de-mongodb-pone-en-riesgo-varios-sitios-web/>
- <http://blog.elevenpaths.com/2014/10/como-funcionan-las-mongodb-injection.html>
- https://www.redeszone.net/2015/02/11/40-000-bases-de-datos-mongodb-abiertas-en-internet/?utm_source=related_posts&utm_medium=widget