Open DB2

1. INTRODUCCIÓN

DB2 es una familia de productos de sistema de gestión de bases de datos relacionales (RDBMS) de IBM que sirven a varias plataformas de sistemas operativos. Es un motor de base de datos relacional que integra XML de manera nativa, lo que IBM ha llamado pureXML, que permite almacenar documentos completos dentro del tipo de datos xml para realizar operaciones y búsquedas de manera jerárquica, e integrarlo con búsquedas relacionales.

La automatización es una de sus características más importantes, ya que permite eliminar tareas rutinarias y permitiendo que el almacenamiento de datos sea más ligero, utilizando menos hardware y reduciendo las necesidades de consumo de alimentación y servidores.

La memoria se ajusta y se optimiza el rendimiento del sistema. Permite resolver problemas de forma automática e incluso adelantarse a su aparición.

2. RIESGO

Este servicio puede exponer información del cliente y además puede utilizarse en ataques de amplificación UDP.

La Vulnerabilidad en IBM DB2 para Unix, Linux y productos Windows server puede permitir el envío de información arbitraria al Fast Communications Manager (FCM) para provocar una denegación de servicio del servidor.

La vulnerabilidad en los productos IBM DB2 listados a continuación permite a un atacante remoto autenticado provocar una denegación de servicio. La vulnerabilidad existe en el Fast Communications Manager (FCM), el cual es utilizado para comunicaciones entre diferentes nodos en una base de datos particionada y entre miembros en una configuración pureScale. Una configuración single node no es vulnerable.

IBM® DB2® Enterprise Server Edition
IBM® DB2® Advanced Enterprise Server Edition

La vulnerabilidad no es aplicable a distribuciones anteriores a v10.1

3. DETECCIÓN

El reporte de “Open DB”” se basa en peticiones UDP al puerto 523 de servidores con direcciones IPv4, si DB2 está habilitado a internet como respuesta se verá información DB2. Para verificar esta vulnerabilidad se puede utilizar el siguiente comando:

```
nmap -sU -p 523 --script db2-discover [IP]
```

INFORMACIÓN DE LOS CAMPOS DEL REPORTE:

Campo	Descripción
Vulnerabilidad	Hace referencia al nombre de la vulnerabilidad
Dirección IP	Dirección IP del dispositivo en cuestión
timestamp_EcuCERT	Fecha y hora de comprobación de EcuCERT en GMT -5
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.
as_name	Nombre del ASN al que pertenece la dirección IP
timestamp	Fecha y hora de comprobación en UTC+0
ip	Dirección IP del dispositivo en cuestión.
protocol	Protocolo de respuesta. (siempre UDP)
port	Puerto del cual vino la respuesta DB2 provino. (usualmente 523)
hostname	DNS reverso del host.
tag	Siempre será DB2.
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.
db2_hostname	Es el nombre de host auto-reportado que se devuelve en la respuesta DB2RETADDR.
servername	El nombre del servidor DB2 que también incluye el nombre DB2RETADDR. Puede o no coincidir con el campo db2_hostname.
size	Payload de respuesta en bytes, incluyendo la cabecera UDP.

4. ACCIONES RECOMENDADAS

Para evitar este tipo de vulnerabilidad se recomienda actualizar los parches, los packs de parches DB2 pueden ser descargados de http://www-01.ibm.com/support/docview.wss?uid=swg27007053.

5. REFERENCIAS

- https://www.shadowserver.org/wiki/pmwiki.php/Services/Open-DB2
- http://searchdatacenter.techtarget.com/es/definicion/DB2
- https://www.certsi.es/alerta-temprana/avisos-seguridad/vulnerabilidad-denegacion-servicio-db2-unix-linux-fast-communications-manager-windows-20131002
- http://www-01.ibm.com/support/docview.wss?uid=swg21650231