SPN SOFTWARE

DECLARACION

VULNERABILIDAD LOG4J FLOW – APACHE –

21-diciembre-2021

La falla Log4j, revelada por Apache la semana pasada, permite a los atacantes ejecutar código de forma remota en una computadora objetivo, lo que significa que pueden robar datos, instalar malware o tomar el control. Algunos ciberdelincuentes han instalado software que utiliza un sistema pirateado para extraer criptomonedas, mientras que otros han desarrollado malware que permite a los atacantes secuestrar computadoras para asaltos a gran escala en la infraestructura de Internet.

Declaraciones de SPN:

SPN Software cuenta con modelos de Business Intelligence (BI) utilizando la herramienta Pentaho BI Suite modalidad Comunitaria. El software Pentaho y sus versiones inferiores a la 8.3 tienen riesgos con esta vulnerabilidad encontrada.

Declaraciones de Pentaho/Hitachi:

Vulnerabilidades log4j 1 y log4j 2 encontradas en CVE-2021-4104, CVE-2021-44228 y CVE-2021-45046

Hitachi Vantara es consciente de las vulnerabilidades antes mencionadas junto con la comunidad. Cualquier cambio en la estrategia de mitigación que se enumera a continuación se actualizará en este artículo.

Software Pentaho:

CVE-2021-4104 Mitigación para Pentaho:
Esta vulnerabilidad no está presente en nuestras versiones actuales de Pentaho totalmente compatibles, ya que no usamos las clases que son vulnerables de forma predeterminada.

Sin embargo, en respuesta al CVE-2021-44228 publicado recientemente, los equipos de ingeniería de Hitachi Vantara han realizado pruebas exhaustivas en nuestro software lanzado, incluido Pentaho.

Para el caso de uso de Pentaho, la vulnerabilidad solo se presentaría si:

Se está utilizando Java 8u120 ó anterior. (Nota: el software Pentaho es compatible con Java 8u251 desde v8.3).

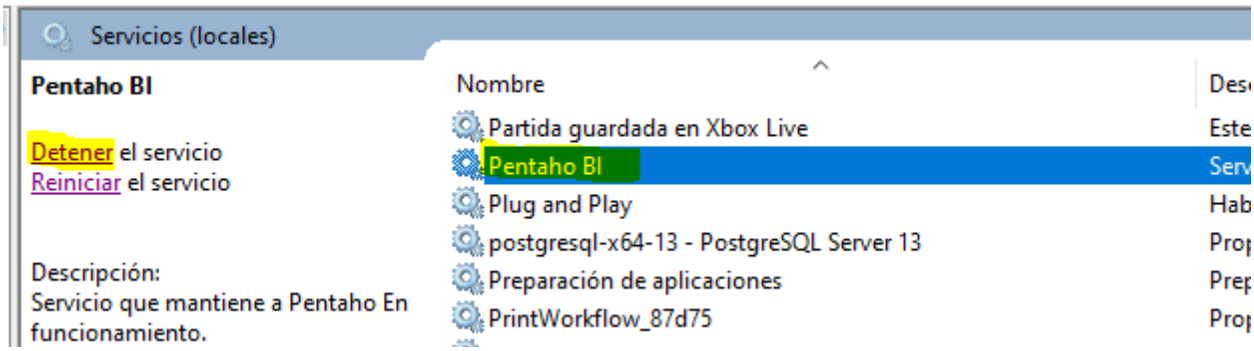
Plan de Acción:

#1. A todo cliente con instalación de Pentaho BI v8.2 ó inferior, proceder de forma inmediata a:

Detener el servicio de Pentaho.

Paso #1. Buscamos la opción Servicios o Services dependiendo el idioma.

Paso #2. Seleccionamos el servicio Pentaho BI- > Clic a detener o Stop.



En caso de no tener el servicio instalado, seguimos estos pasos.

Paso #1: Revisamos si en la barra de tareas tenemos el programa TomCat ejecución.

Paso #2: Cerramos.

#2. Coordinar junto al equipo de BI de SPN Software la actualización de Pentaho a su versión más reciente, la v8.3, que ya mitiga la vulnerabilidad.