



SPN SOFTWARE DECLARACION

VULNERABILIDAD LOG4NET 1.2.10 LOCALSYSLOGAPPENDER FORMAT STRING – APACHE – 09-octubre-2023

Una vulnerabilidad ha sido encontrada en Apache log4net 1.2.10 y clasificada como crítica. Una función desconocida del componente LocalSyslogAppender es afectada por esta vulnerabilidad. A través de la manipulación de un input desconocido se causa una vulnerabilidad de clase format string. Esto tiene repercusión sobre la confidencialidad, integridad y disponibilidad.

La vulnerabilidad fue publicada el 2006-03-07 por Sebastian Krahmer con identificación 19241 con un advisory (Secunia) (confirmado). El advisory puede ser descargado de secunia.com. La vulnerabilidad es identificada como CVE-2006-0743. Es fácil de explotar. El ataque puede ser realizado a través de la red. La explotación no requiere ninguna forma de autenticación. No se conoce los detalles técnicos ni hay ningún exploit disponible.

Fue declarado como proof-of-concept. Para el scanner Nessus se dispone de un plugin ID 27343 (openSUSE 10 Security Update : log4net (log4net-2211)), que puede ayudar a determinar la existencia del riesgo analizado.

Las versiones de Apache log4net anteriores a la 2.0.10 no deshabilitan las entidades externas XML al analizar los archivos de configuración de log4net. Esto permite ataques basados en XXE en aplicaciones que aceptan archivos de configuración log4net controlados por el atacante.

Una actualización a la versión 2.0.10 o superior elimina esta vulnerabilidad.

Declaraciones de SPN:

SPN Software cuenta con plataformas web (Autoservicio, Evaluación del Desempeño, Capacitación) que usan esta librería, por lo que tienen riesgos con esta vulnerabilidad encontrada.

Declaraciones de APACHE:

CVE-2018-1285 Las versiones de Apache log4net anteriores a la 2.0.10 no deshabilitan las entidades externas XML al analizar los archivos de configuración de log4net. Esto permite ataques basados en XXE en aplicaciones que aceptan archivos de configuración log4net controlados por el atacante.

Plan de Acción:

#1. A todo cliente con instalación de plataformas web (Autoservicio, Evaluación del Desempeño, Capacitación), proceder de forma inmediata:

Desde nuestra plataforma de Mesa de Ayuda <https://hd.spn.com.do/> proceder a crear un caso, solicitando coordinar la actualización de las plataformas web de SPN.