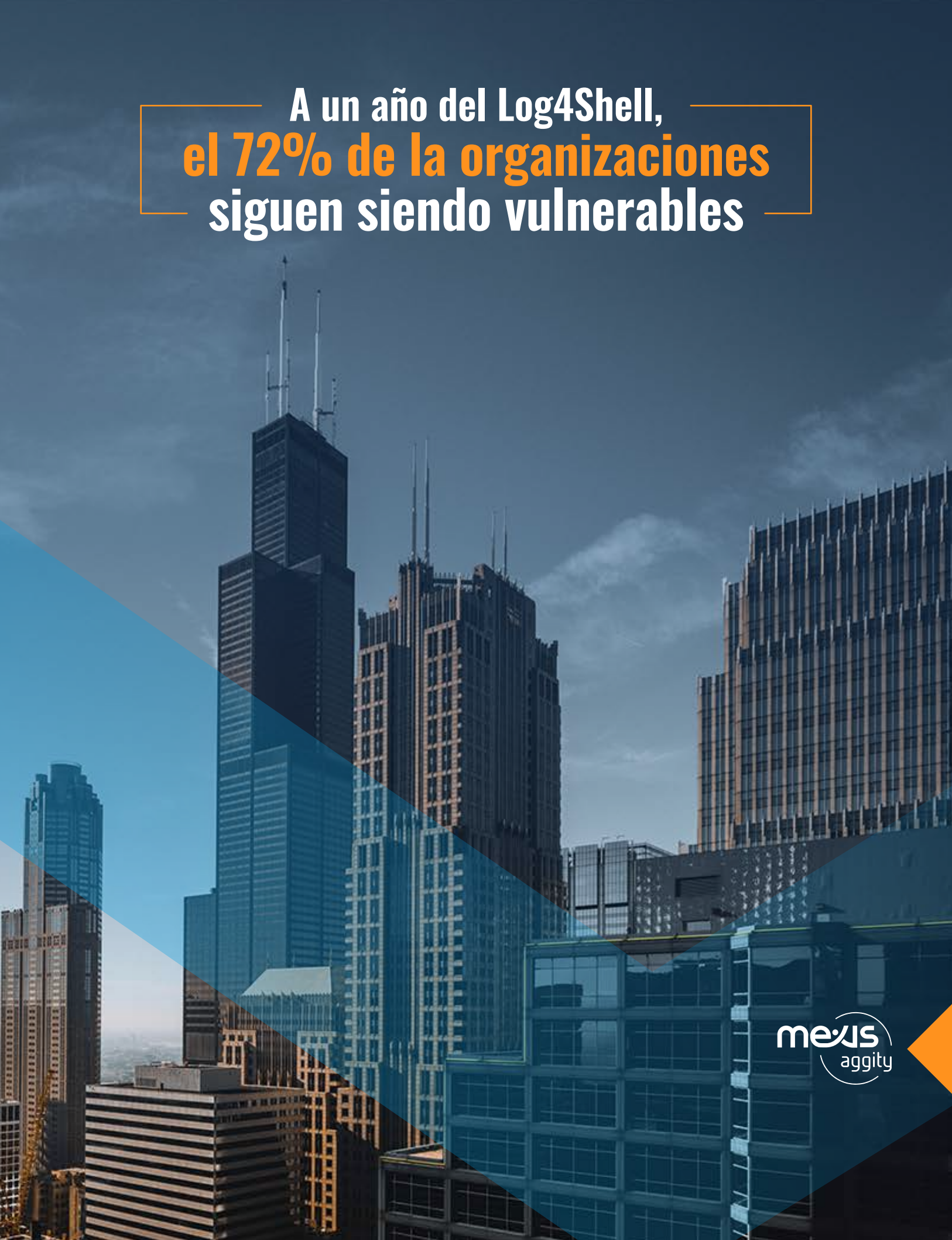
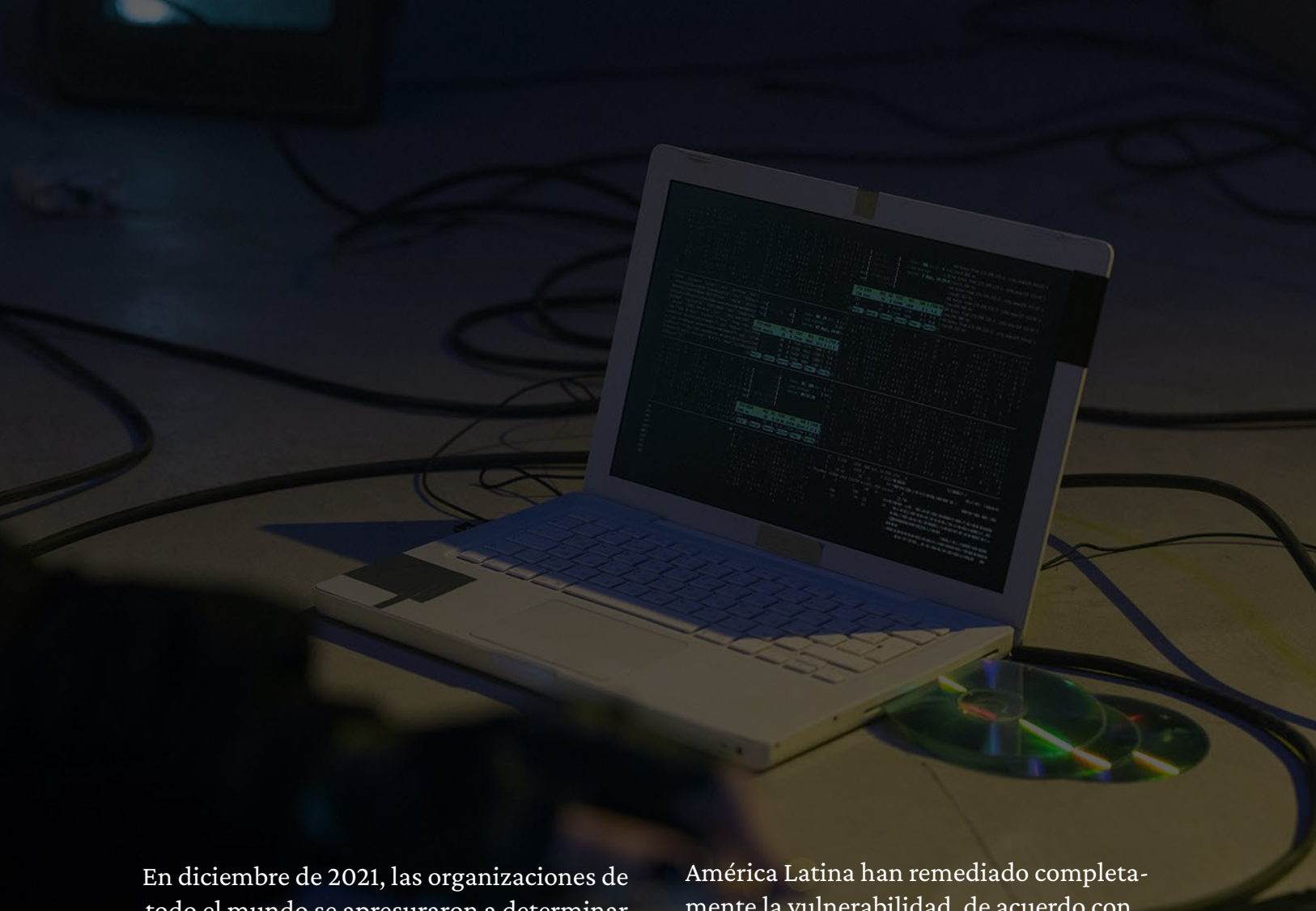
A un año del Log4Shell, el 72% de la organizaciones siguen siendo vulnerables



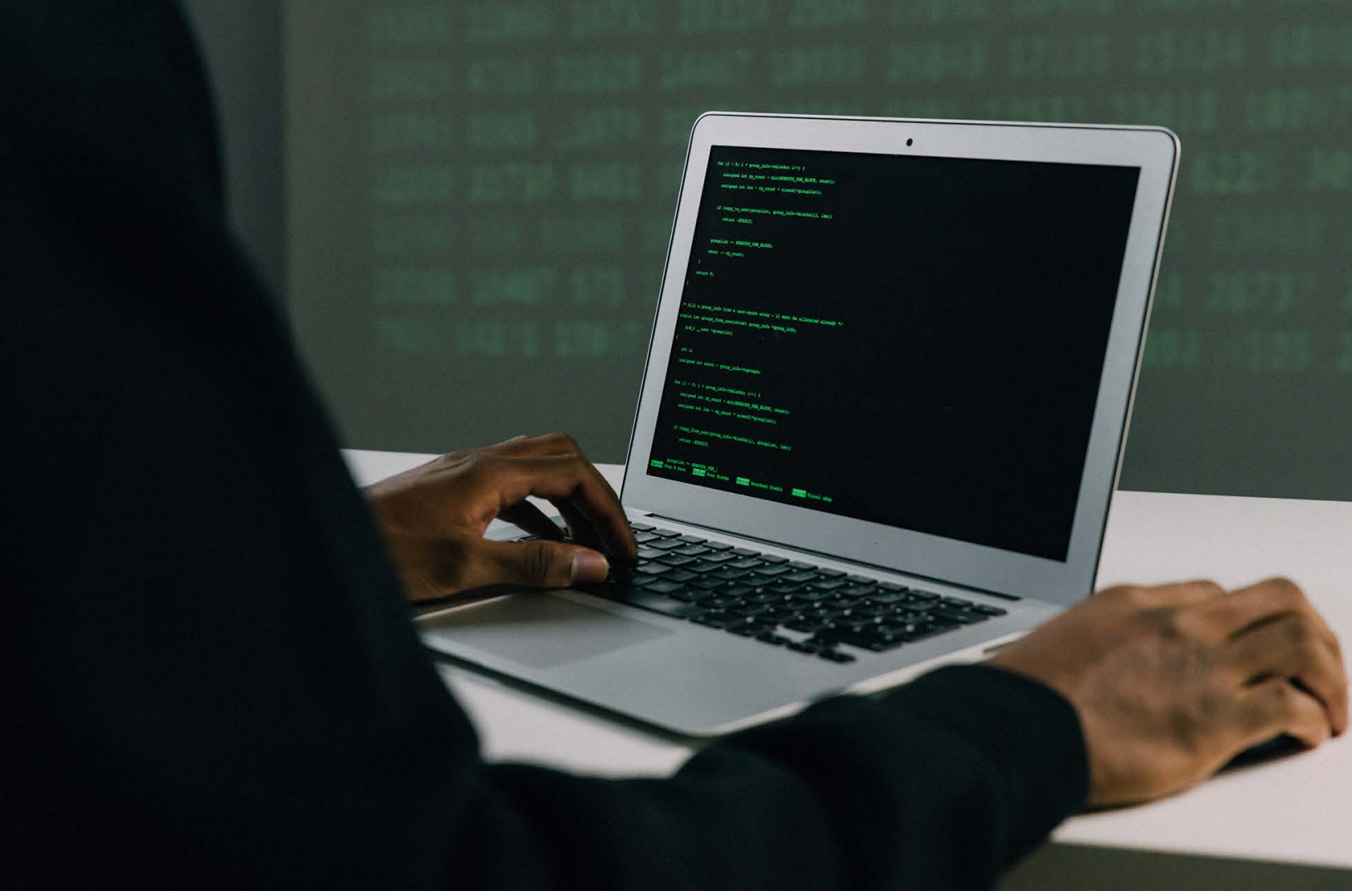


En diciembre de 2021, las organizaciones de todo el mundo se apresuraron a determinar el riesgo de la vulnerabilidad Log4j, conocida como Log4Shell, “una de las más críticas de la última década”, según lo publicado en CIO México.

En las semanas posteriores a la divulgación de esta vulnerabilidad –nombrada así por estar presente en Apache Log4j, una importante biblioteca de registro de código abierto de Apache las organizaciones reasignaron recursos de manera significativa e invirtieron decenas de miles de horas en esfuerzos de identificación y remediación. Un año después, el 72% de las organizaciones siguen siendo vulnerables, y sólo el 21% de éstas en América Latina han remediado completamente la vulnerabilidad, de acuerdo con estudio.

Este estudio de telemetría indica que en diciembre del año pasado, uno de cada 10 activos era vulnerable a Log4Shell, lo cual incluye a servidores, aplicaciones web, contenedores y dispositivos de Internet de las Cosas. Para octubre de 2022, se reportaron mejoras, según el documento, con un 2.5% de los activos vulnerables. Sin embargo, casi un tercio (29%) de estos activos tuvieron recurrencias de Log4Shell después de que se logró la remediación completa.

Sin embargo, casi un tercio (29%) de estos activos tuvieron recurrencias de Log4Shell después de que se logró la remediación completa.



¿A QUÉ SE DEBE ESTO?

La remediación completa es muy difícil de lograr para una vulnerabilidad que es tan generalizada, por eso es importante tener en cuenta que la remediación de vulnerabilidades no es un proceso de una vez.

Si bien una organización puede haber sido remediada por completo en algún momento, ya que agregaron nuevos activos a sus entornos, es probable que se encuentren con Log4Shell una y otra vez. “Erradicar Log4Shell es una batalla continua que requiere que las organizaciones evalúen continuamente sus entornos en busca de fallas, así como otras vulnerabilidades conocidas.

OTROS HALLAZGOS

En el estudio se reporta que el 28% de las organizaciones de todo el mundo han remediado Log4Shell por completo a partir del 1 de octubre de 2022, una mejora de 14 puntos desde mayo de 2022. Cabe señalar que el 53% de las organizaciones eran vulnerables a Log4j durante el período de tiempo del estudio, lo que subraya la naturaleza omnipresente de Log4j y los esfuerzos continuos necesarios para remediar, incluso si se logró previamente una remediación completa.

No obstante, el documento notifica que a partir de octubre de 2022, el 29% de los activos vulnerables vio la reintroducción de Log4Shell después de que se logró la remediación completa.

Fuente de información: cio.com.mx