La Apache Software Foundation (ASF) lanzó el martes nuevos parches para contener una falla de ejecución de código arbitrario en Log4j, que podría ser abusada por los atacantes para ejecutar código malicioso en los sistemas afectados, lo que la convierte en la quina vulnerabilidad de seguridad descubierta en la herramienta en tan solo un mes.

Rastreada como CVE-2021-44832, la vulnerabilidad tiene una gravedad de 6.6 en una escala de 10, e impacta todas las versiones de la biblioteca de registro desde 2.0-alpha7 a 2.17.0 con la excepción de 2.3.2 y 2.12.4.

Aunque las versiones 1.x de Log4j no se ven afectadas, se recomienda a los usuarios actualizar a Log4j 2.3.2 (para Java 6), 2.12.4 (para Java 7) o 2.17.1 (para Java 8 y posterior).

> *«Las versiones 2.0-beta7 a 2.17.9 de Apache Log4j2 (excluidas las versiones de corrección de seguridad 2.3.2 y 2.12.4) son vulnerables a un ataque de ejecución remota de código (RCE) donde un atacante con permiso para modificar el archivo de configuración de registro puede construir una configuración mediante un JDBC Appender de una fuente de datos con referencia a un URI JNDI que pueden ejecutar código remoto. Este problema se soluciona limitando los nombres de las fuentes de datos JNDI al protocolo java en las versiones 2.17.1, 2.12.4 y 2.3.2 de Log4j2»*, dijo la ASF en un aviso.

Aunque la ASF no otorgó créditos por el problema, el investigador de seguridad de Checkmarx, Yaniv Nizry, reclamó el crédito por informar la vulnerabilidad a Apache el 27 de diciembre.

> *«La complejidad de esta vulnerabilidad es mayor que la de CVE-2021-44228 original, ya que requiere que el atacante tenga control sobre la configuración. A diferencia de Logback, en Log4j hay una función para cargar un archivo de configuración remota o para configurar el registrador a través del código, por lo que se podría lograr una ejecución de código arbitrario con un ataque MiTM, la entrada*

> *del usuario termina en una variable de configuración vulnerable, o modificando el archivo de configuración»,* dijo Nizry.

Con la última solución, los encargados del mantenimiento del proyecto abordaron un total de cuatro problemas en Log4j desde que la vulnerabilidad Log4Shell se dio a conocer a inicios de diciembre, sin mencionar una quinta vulnerabilidad que afecta a las versiones Log4j 1.2 que no se solucionará:

- CVE-2021-44228 (puntuación CVSS de 10.0): Una vulnerabilidad de ejecución remota de código que afecta a las versiones de Log4j de 2.0-beta9 a 2.14.1 (corregida en la versión 2.15.0).
- CVE-2021-45046 (puntuación CVSS de 9.0): Una fuga de información y una vulnerabilidad de ejecución remota de código que afecta a las versiones de Log4j de 2.0-beta9 a 2.15.0, excluyendo 2.12.2 (corregido en la versión 2.16.0).
- CVE-2021-45105 (puntuación CVSS de 7.5): Una vulnerabilidad de denegación de servicio que afecta a las versiones de Log4j de 2.0-beta9 a 2.16.0 (corregida en la versión 2.17.0).
- CVE-2021-4104 (puntuación CVSS de 8.1): Una falla de deserialización no confiable que afecta a la versión 1.2 de Log4j (no hay solución disponible; actualizar a la versión 2.17.1).

Esto se produce al tiempo que las agencias de inteligencia de Australia, Canadá, Nueva Zelanda, Reino Unido y Estados Unidos emitieron una advertencia conjunta sobre la explotación masiva de múltiples vulnerabilidades en la biblioteca de software Log4j de Apache por parte de hackers.