Log4Shell Vulnerability

Zero-Day in the Log4j Java library

ثغرة أمنية خطيرة في مكتبة Log4j، وهي مكتبة Java تم تطويرها من قبل Apache Software Foundation وهي مفتوحة المصدر، يتم تضمينها في أطر مخدمات الويب Apache مثل:

Apache Struts2, Apache Solr, Apache Druid, Apache Flink, Apache Swift

تُستخدم على نطاق واسع لتسجيل رسائل الخطأ في التطبيقات، حيث يتم استخدامها في تطبيقات برامج المؤسسات، بما في ذلك تلك التطبيقات المخصصة التي طورتها الشركات داخليًا، وتشكل جزءاً من العديد من خدمات الحوسبة السحابية وتطبيقات الويب وخدمات البريد الإلكتروني، مما يعني أن هنالك مجموعة واسعة من البرامج التي قد تكون معرضة للخطر من محاولات استغلال هذه الثغرة.

تم تصنيف هذه الثغرة من قِبل المنظمات المعنيّة بتصنيف الثغرات تحت بالرمز (CVE-2021-44228) بدرجة خطورة عالية وبمجموع نقاط 10 من 10.

التأثير

يسمح الاستغلال الناجح للثغرة للمهاجمين بما يلي:

- تنفيذ تعليمات برمجية تعسفيّة عن بُعد Remote Code Execution RCE

– الوصول غير المرخّص إلى المخدمات وغيرها من التجهيزات المتأثرة مع إمكانية التحكم الكامل بالأنظمة System Compromised

– تثبيت أدوات تحكم عن بعد على الأنظمة المعرّضة لاستغلال هذه الثغرة، وهو أمر قد يسمح للمهاجمين بالاستيلاء على أسماء المستخدمين وكلمات المرور وغيرها من البيانات الهامة.

– تثبيت برامج تعدين العملات الرقمية المشفرة.

الإصدارات المتأثرة

تتأثر جميع الأنظمة والخدمات التي تستخدم Java logging library, Apache Log4j2 بين الإصدارين 2.0 و 2.14.1، بما في ذلك العديد من الخدمات والتطبيقات المكتوبة بلغة Java.

الحلول

يجب وعلى وجه السرعة تحديث وترقية إصدارات Log4j إلى log4j-2.15.0-rc1
بالنسبة للإصدارات Log4j 2.10.0 والإصدارات الأحدث حتى ما قبل 2.15.0 فيمكن التخفيف من احتمال الاستغلال عن طريق تعيين خاصية النظام "log4j2.formatMsgNoLookups" to "true"،

أو إزالة JndiLookup class من Classpath

مع التأكيد بأن التحديث والترقية إلى الإصدارات غير المتأثرة بالثغرة هو الإجراء الأفضل والأكثر أمناً.

توصيات إضافية:

- التدقيق والبحث ضمن الأجهزة الشبكية على المكتبة المتأثرة بالثغرة Log4Shell
- مراقبة عمليات التثبيت الناجحة أو محاولات تثبيت المكتبة Log4j ضمن الحواسب ومحطات العمل والمخدمات وغيرها من الأجهزة الشبكية، من خلال وسائط الحماية والمراقبة ذات الصلة وإصدار التحذيرات المناسبة بشأن ذلك.
- تثبيت جدران حماية تطبيقات الويب WAFs وإعدادها بحيث تحوي قواعد عمل مخصصة Customed Rules تقوم بالتركيز على كل ما يتعلق بالمكتبة Log4j، كمحاولات البحث والمسح ومحاولات الهجوم باستغلال هذه الثغرة.

مراجع

- https://tinyurl.com/5fbef64u
- https://tinyurl.com/2p94t5h3
- https://tinyurl.com/49f2hzxb
- https://tinyurl.com/27dyktb3
- https://tinyurl.com/yckkcwxa

إعداد

دائرة الإستجابة للطوارئ المعلوماتية

م. سُليمه كنينه

إشراف

رئيس دائرة الدراسات والأبحاث

أ. ماجد اسماعيل

15 كانون الأول 2021