PERINGATAN KEAMANAN
KERENTANAN ZERO-DAY PADA APACHE JAVA LOGGING LIBRARY LOG4J (CVE-2021-44228)

RINGKASAN

1. Pada tanggal 9 Desember 2021, periset keamanan menemukan adanya kerentanan zero-day yang diberi nama CVE-2021-44228 pada pustaka Apache Java Logging Library atau yang umum dikenal dengan log4j.
2. Adapun versi dari Log4j yang terdampak oleh kerentanan ini adalah sistem elektronik yang menggunakan Apache Log4j antara versi 2.0 sampai dengan 2.14.1. Berdasarkan CVSS Score 3.0, nilai kerentanan ini memiliki nilai 10.0 atau dikategorikan sebagai **KRITIKAL**. Eksploitasi dari kerentanan ini memungkinkan penyerang dapat mengambil alih penuh server yang terdampak.
3. Seluruh pengguna yang menggunakan versi yang terdampak direkomendasikan untuk melakukan pemutakhiran ke versi terbaru atau melakukan langkah mitigasi sebagaimana direkomendasikan pada dokumen ini.

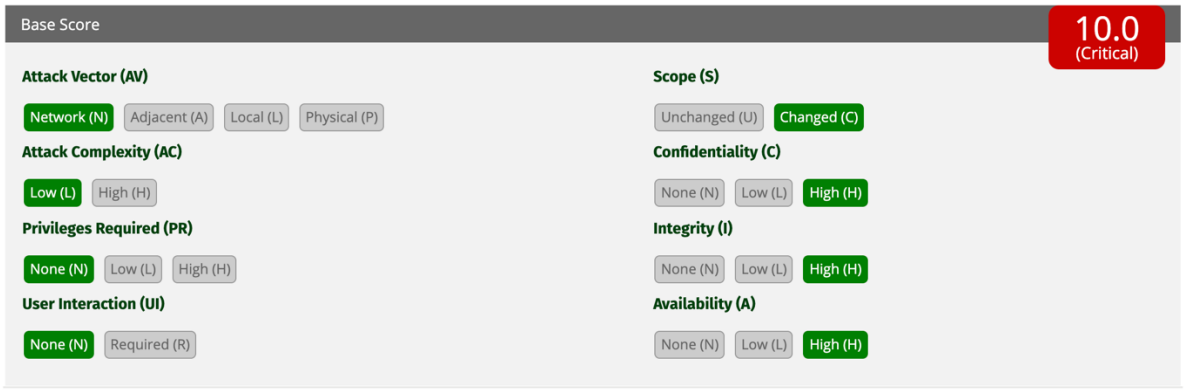
PENDAHULUAN

Pada tanggal 9 Desember 2021, periset keamanan menemukan adanya kerentanan zero-day yang diberi nama CVE-2021-44228 pada pustaka Apache Java Logging Library atau yang umum dikenal dengan log4j. ***Proof of Concept*** **(PoC) exploit dari kerentanan tersebut juga telah tersedia secara bebas**. Eksploitasi dari kerentanan ini memungkinkan penyerang dapat mengambil alih penuh server yang terdampak.

NILAI KERENTANAN

Berdasarkan CVSS Score 3.0, nilai kerentanan ini memiliki nilai : 10.0 atau dikategorikan sebagai **KRITIKAL**.

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H



VERSI YANG TERDAMPAK

Adapun versi dari Log4j yang terdampak oleh kerentanan ini adalah sistem elektronik yang menggunakan Apache Log4j antara versi 2.0 sampai dengan 2.14.1. Hal ini berpotensi pula terdampak pada aplikasi dan layanan yang dikembangkan dengan bahasa pemrograman Java yang menggunakan pustaka ini.

PANDUAN MITIGASI KERENTANAN

Untuk mencegah eksploitasi kerentanan ini direkomendasikan kepada pemilik sistem elektronik yang menggunakan versi Apache log4j yang terdampak untuk melakukan langkah-langkah berikut:

1. Jika versi Apache log4j yang digunakan sebelum versi 2.10, direkomendasikan untuk memutakhirkan Apache log4j yang digunakan ke versi log4j-2.15.0 atau terbaru.
2. Langkah mitigasi yang dapat dilakukan terkait dengan hal ini apabila sistem elektronik yang digunakan merupakan versi 2.10 atau terbaru yakni:
   Mengkonfigurasi `log4j2.formatMsgNoLookups` menjadi **`true`** dengan menambahkan baris berikut pada JVM command untuk memulai aplikasi

   `"-Dlog4j2.formatMsgNoLookups=True”`

   atau mengkonfigurasi nilai environment variabel

   `LOG4J_FORMAT_MSG_NO_LOOKUPS` menjadi `true`

3. Apabila versi Apache log4j yang digunakan mulai dari versi dari 2.0-beta9 hingga 2.10.0, langkah mtigasi yang dapat dilakukan yakni dengan `JndiLookup class` dari classpath:

   ```
   zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
   ```

4. Menonaktifkan JNDI. Misalkan dengan menambahkan `Spring.jndi.ignore=true` yang digunakan pada `spring.properties`

5. Direkomendasikan untuk menggunakan JDK versi yang lebih tinggi dari 11.0.1, 8u191, 7u201, 6u211 atau yang lebih terbaru.
6. Jika memungkinkan lakukan pembatasan terhadap sistem elektronik yang terdampak agar tidak dapat diakses melalui internet.
7. Lakukan langkah perlindungan lainnya dengan memutakhirkan rules deteksi pada perimeter keamanan WAF yang digunakan.

REFERENSI

[1]. Log4j RCE 0-day actively exploited. https://www.cert.govt.nz/it-specialists/advisories/log4j-rce-0-day-actively-exploited

[2]. Apache Log4j Security Vulnerabilities. https://logging.apache.org/log4j/2.x/security.html

[3]. AusCERT Security Bulletin. https://auscert.org.au/bulletins/ASB-2021.0244.2

[4]. Log4Shell: RCE 0-day exploit found in log4j2, a popular Java logging package. https://www.lunasec.io/docs/blog/log4j-zero-day/