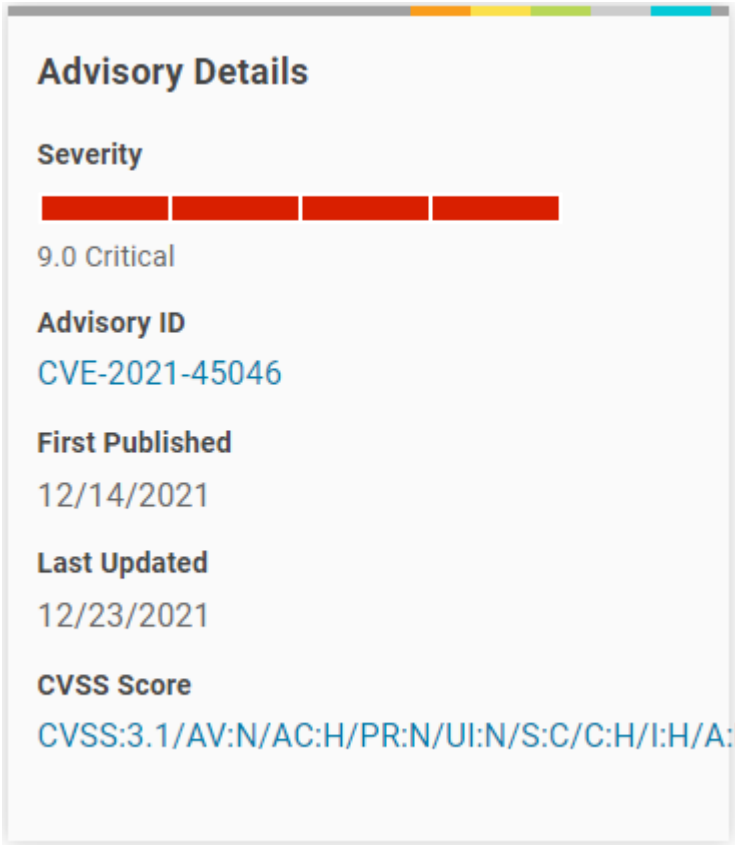
Security Advisory Summary



It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allow attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $${ctx:loginId}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.

December 13, 2021, the Apache Software Foundation released Log4j 2.16.0 to disable default access to JNDI lookups and limits the protocols by default to only Java, LDAP, and LDAPS and limits the LDAP protocols to only accessing Java primitive objects to resolve a vulnerability which could leave an affected system open to a denial-of-service attack (CVE-2021-45046).

December 17, 2021, the Apache Software Foundation released Log4j 2.17.0 to resolve a Denial-of-Service vulnerability in Apache Log4j2 versions 2.0-alpha1 through 2.16.0, which did not protect from uncontrolled recursion from self-referential lookups (CVE-2021-45105).

December 21, 2021, the National Institute of Standards and Technology (NIST) upgraded CVE-2021-45046 from a severity of 3.7 (Low) as originally reported on December 14, to 9.0 (Critical).

For more information on this CVE and guidance to mitigate this vulnerability, please visit our security advisory for CVE-2021-44228.