Datadog, Inc.
620 8th Avenue, 45th Floor
New York, NY 10018
(866) 329-4466
www.datadoghq.com

December 10, 2021

As you may already be aware, it was recently announced that log4j, a popular logging library used by the majority of Java applications, is vulnerable to remote code execution.

We have not found any evidence of attackers leveraging this vulnerability against us. To be safe, Datadog has taken the necessary steps to update any implementations of log4j. We are writing to provide you with more information about this vulnerability as we know it, and provide recommended steps that you can take to remediate it as part of your overall remediation efforts.

What we know so far

On December 9th, 2021, The Apache foundation released a vulnerability disclosure regarding its log4j library that is widely used by Java applications. The vulnerability can potentially allow an attacker to craft a message that when processed by the library, can trick the system hosting the application to reach out to a remote system and download a compiled Java class that can be executed within the system that received the log entry.

Steps Datadog has Taken

Immediately following the disclosure, Datadog's Information Security team began investigating the impact to our internal systems and our customers. We identified a number of services leveraging the impacted version of log4j and these were quickly remediated by our engineering teams.

In addition, we also identified that the JMX monitoring component of our Agent software also leverages an impacted version of log4j. We are releasing a new version of the agent (7.32.2) in the next 48 hours, which prevents the vulnerability from being exploited. We encourage you to update to this version when available. Please note that the impacted log4j library is still included with the agent, but we have taken the precautions recommended by the Apache foundation so that the vulnerable logic is disabled.

Please keep this in mind as your vulnerability scanners may pick up this version during your scans. Our teams are working on removing the dependency of log4j in a future release of the Agent.

Finally, if for any reason you cannot update the Datadog agent or any of your Java applications, we highly recommend that you set the following property as part of your JVM start up configuration.

```
-Dlog4j2.formatMsgNoLookups=True
```

Truly,
Emilio Escobar
Chief Information Security Officer
emilio.escobar@datadoghq.com