Namirial’s response to Apache Log4j vulnerabilities

On December 9, 2021, Namirial was made aware of a security vulnerability impacting the Apache Log4j 2 Java library dubbed Log4Shell (or LogJam) reported with CVE-2021-44228. This vulnerability, which is being widely exploited by a growing set of threat actors, presents an urgent challenge to network defenders given its broad use. We immediately mobilized to understand and remediate any exposures that we might have to this vulnerability.

We immediately started investigating and taking action for Namirial as an enterprise, Namirial products and Namirial services that may be potentially impacted, and will continually publish information to help customers detect, investigate and mitigate attacks, if any, to their Namirial products and services.

**** Update 15/12/2021 ****

Subsequently to the publication of the CVE-2021-44228 an additional vulnerability has been published with CVE-2021-45046. Namirial confirms that the investigations have been extended on December 14 even to this vulnerability.

**** Update 20/12/2021 ****

Subsequently to the publication of the CVE-2021-45046 an additional vulnerability has been published with CVE-2021-45105. Namirial confirms that the investigations have been extended on December 18 even to this vulnerability.

**** Update 29/12/2021 ****

Subsequently to the publication of the CVE-2021-45105 an additional vulnerability has been published with CVE-2021-44832. Namirial confirms that the investigations have been extended on December 29 even to this vulnerability.

Namirial Enterprise

Namirial is continuing to inventory our products and systems potentially impacted by these vulnerabilities. As necessary, we are updating to Log4j version 2.17.1, which fixes all the vulnerabilities reported till December 29, and applying mitigations in the interim, even in cases where additional control layers such as network controls and web application firewalls prevent exploitation of these vulnerabilities. Anyway, due to the criticality of the services provided, Namirial does not share documents or information relating to its security systems and controls to respond to the requests for additions and clarifications regarding the security of information made by third parties, be they Customers, Suppliers and/or Partners.

Namirial Software and Systems Products

Namirial understands the critical nature of these issues and the need to provide a complete response for all Namirial products as soon as possible. Namirial development teams are working around the clock to complete the investigation and, as needed, any remediation on this vulnerability.

Namirial follows ethical vulnerability disclosure management practices. This means that Namirial does not confirm or otherwise disclose vulnerabilities externally, even to individual customers, until a fix or remediation is available. If a Namirial Software or Systems product is impacted, there will be a bulletin posted on the Namirial website as soon as a remediation or fix becomes available. Such on-premise Namirial products will then need to be updated by the customer as defined within the related security bulletin.

Namirial Support & Delivery

Namirial will continue to work directly with its clients in support of the remediation of custom applications and services through its normal delivery center and platform support processes.

Namirial Cyber Security

The Namirial team of hackers, responders, researchers, intelligence analysts and investigators are actively engaged in the response to Log4Shell.

Namirial Cloud and as-a-Service Products

For Namirial Cloud services, Namirial is remediating managed as-a-service Cloud offerings as applicable, even in cases where additional control layers such as network controls and web application firewalls prevent exploitation of this vulnerability.

Clients who have deployed their own applications using the Namirial Infrastructure as a Service, or virtual and bare metal machines are responsible for remediating any Log4j vulnerabilities running on those services.

For the portion of Namirial Cloud services using Java technologies, Namirial is continuing to assess and remediate any remaining services using Log4j and validate that mitigating controls remain effective.

Products not Impacted

Namirial’s analysis are still in place to determine which of the above vulnerabilities impacts our products. Here a list of Products not Impacted on the basis of latest analysis. This list is not final and continuously updated.