

Log4j Java Vulnerability Update - December 23, 2021

Medidata's Information Security team has been continuously monitoring and refining our detective and preventive systems to ensure that there is no exploitation of the Log4j vulnerabilities, and alert on any activity that may result from a vulnerability being exploited.

Medidata has identified no cases of exploitation; and our cloud, perimeter and host based protections are actively defended from all published log4j vulnerability based attacks.

We feel that we have the proper monitoring and response capabilities that would allow us to detect any such attack within the environment, and respond accordingly.

With our perimeter security preventive controls and monitoring in place, Medidata has conducted a thorough analysis of the following systems for any use of log4j; whether utilized as part of a Medidata developed product or as part of a utilized tool/service:

- Customer facing products
- Infrastructure hosting customer facing products
- Code repositories
- Infrastructure hosting Medidata (internal) business utilities
- Business service providers

In all cases where log4j is utilized, the product or services have either been upgraded to utilize log4j Version 2.16.0, or testing and release is underway as an emergency update.

This includes not only Medidata developed products, but also required reviewing relevant suppliers. Version 2.17.0 will be addressed after the critical vulnerabilities are closed as part of the normal update cycle.

The original total population of log4j vulnerable libraries was less than 4% of our total code base, none of which are in high risk products (iMedidata/CloudAdmin, Rave EDC, Rave RTSM/Balance, or any of our data science products).

All subprocessors who interact or protect Covered Data have been updated; or the provided services disabled until the update is complete. The initial work updating the impacted libraries for multi-tenant services is complete; follow through on the remaining legacy single instance products remaining will be performed as soon as feasible.

To help protect the data that you and your patients trust us with, Medidata has strong mitigations at our perimeter and on each server, providing multiple layers of security. Since the initial notification on the vulnerability, Medidata has been aggressively addressing the issue through additional patching and implementation of additional controls at the network, server and application levels.

We are approaching this in a controlled, measured and precise manner as part of our NIST 800-53 based approach on vulnerability management and change control.

At this point, Medidata is confident that the controls which are protecting the data that you trust us with are intact, and that we have sufficient monitoring within the environment to detect problems before they progress.

Log4j Java Vulnerability Addendum - December 13, 2021

The Dassault Systèmes leadership has invested heavily in terms of focus, funding and resources to protect the data that our customers and their patients trust us with.

The log4j “LogJam” java logger vulnerability is enormously impactful, requiring aggressive countermeasures which include firewall modifications, load balancer enhancements, system updates and configuration changes.

The observer volume of malicious traffic is up over 400% in the last 72 hours, and the infrastructure is managing this as designed, without any issues.

We are receiving some malformed traffic attempting to enter the Medidata Clinical Cloud from some Sites.

The perimeter controls, as designed, are blocking this traffic, preventing it from entering the environment and creating unauthorized access.

It is possible that some sites have taken the initiative to scan the MCC environment; which would trigger the same result.

As we cannot distinguish between well intended security scanning versus malicious traffic, we block all such attempts to gain access.

We specifically prohibit by policy such customer initiated scans, for the same reason. Details on our security posture, including vulnerability scans are available via self-service at <http://www.mdsol.com/trust>.

In the event of blocking a legitimate entity, the traditional processes through Customer Success will result in a restoration of service, after a brief confirmation of identity.

It’s critically important that the scanning stops prior to that restoration, or that the botnet is cleaned up prior to service, otherwise the blocking will automatically re-instantiate.

We continue our vigil in protecting the integrity and availability of the data that you trust us with, and that the patient relies on.

Logj4 Java Vulnerability on December 10, 2021

Within the Technology arena, weaknesses manifest that may be exploited by a malicious actor, in order to perform unauthorized activities such as inserting ransomware, steal data or perform other malintended activities.

This is a matter of daily operations, as many hundreds of thousands of these kinds of vulnerabilities are discovered every year throughout the world.

In order to continue to deliver treatment safely, the Dassault Systèmes leadership has invested heavily in terms of focus, funding and resources to protect the data that our customers and their patients trust us with.

Part of that is an effective Vulnerability Management Program; which is an enormous undertaking, which requires identifying, classifying, and addressing these weaknesses. Not all vulnerabilities require action, but when they are material, they require brisk and decisive action.

Within the last 72 hours a critical vulnerability to a common tool has been identified, and weaponized by nation states, organized crime and independent actors in order to take advantage of the situation.

The library - "Apache logj4" is part of the Apache web server, is a mechanism to providing logging for a specific set of Java applications. The vulnerability is critical, which means that it grants extraordinary access, it is trivial to take advantage of (requiring only a few lines of code), and is very common in tools and services.

Medidata does use this service in about 4% of our Products, Services and tooling to support them.

To help protect your data, we have strong mitigations at our perimeter and on each server, providing multiple layers of security in the environments that we manage.

At this point, we are comfortable that the controls protecting the data that you trust us with are intact, and that we have sufficient monitoring within the environment to detect problems before they develop.

As strictly a precautionary measure, we are going to patch the affected system as part of an emergency update over the next few days.

We are approaching this in a controlled, measured and precise manner as part of our NIST 800-53 based approach on vulnerability management and change control., and expect it to be transparent to our customers. This activity should be complete this week.