

Date: June 1, 2022
 ZEJP-1301A

Dear Valued Customers

Apache Log4j Vulnerability and Action to be Taken

Thank you very much for your continuous support. Apache announced a critical vulnerability within the Log4j logging library for Java. The official CVSS Base score has been determined as a severity of 10. We have listed affected software products requiring customer action. To address the security vulnerability, users are recommended to install the patch program when available. Please contact your local service office.

Note: As of June 1, 2022, no impact is found on any products outside of the list below.

1) Software Products

Software name	Version	Type	Impact	Patch program
Multi-omics Analysis Package	1.10	LCMS	Yes	1.10SP2
Multi-omics Analysis Package	1.01 or lower	LCMS	Yes	1.01SP1

Note: In Patch Program 1.10 SP1 released earlier, the [Cytoscape] gadget is not supported for the purpose of implementing vulnerability countermeasures.

2) Related Products

Software name	Version	Including software
LC/MS/MS Method Package (Primary Metabolites)	2.0 or higher	Multi-omics Analysis Package
LC/MS/MS Method Package (Cell Culture Profiling)	1.0 or higher	Multi-omics Analysis Package
Metabolites Method Package Suite	1.0	Multi-omics Analysis Package


3) Temporary Measures to be Taken (until the improved program is installed)

If applicable to the products listed in 1) and 2), before using the gadgets [VolcanoPlotGenerator] and [Cytoscape] included in Multi-omics Analysis Package, please be sure to disconnect the computer from the external network. If unable to disconnect, never use the gadgets [VolcanoPlotGenerator] and [Cytoscape]. To check whether the system has the actual impact, please consult your security administrator.

4) Patch Program

The patch program was released on May 30, 2022.

Faithfully yours,



Toshiyuki Kawano
General Manager
Quality Assurance Department
Analytical & Measuring Instruments Division
Shimadzu Corporation