

# Log4j2 vulnerability(CVE-2021-44228) and Astah Products

Last updated: December 16th, 2021

On December 9, 2021, a vulnerability in [Apache Log4j \(CVE-2021-44228\)](#) was identified.

We have performed a thorough investigation and here's the report. We will continue to investigate any potential exposure to this vulnerability and updates this page with findings. So please check back frequently for updates.



## Astah Professional, UML, SysML, GSN and Viewer

None of these products is affected by this vulnerability because they do not use Log4j2.

• • •

## Astah System Safety

Astah System Safety uses Log4j2 only for Excel-export functionality, however we confirm that it is not affected by this vulnerability after a thorough investigation. If you'd like to take log4j file out of the system, please remove log4j-core-2.9.0.jar that is stored in lib folder. Deleting this file does not affect the usage of the product.

• • •

## Plugins

All of the latest versions of [plug-ins](#) are not affected by this vulnerability.

• • •

## Floating License Server

A license server you use for [Astah floating license](#) is not affected by this vulnerability since it does not use Java.

• • •

## Our Websites

[Astah.net](#) (You are on this site), [ChangeVision Members](#) and [Astah blogs](#) are not affected by this vulnerability.

• • •

We are currently investigating the impact to the [M+ Plugin](#) and will update this page as soon as we have the result.

If you have any specific questions related to this event, please [contact us](#).

**Update 16th December 2021 – 10:35 JST**

### Compare Products

Astah Professional  
Astah UML  
Astah System Safety  
Astah SysML  
Astah Community  
Astah Viewer

Plug-ins

### Who We Serve

Students  
Individuals  
Development Teams  
Astah Fans

### Tutorials

Modeling Basics & Best  
Practices  
Support  
Astah API

### Purchasing Astah

Pricing  
Free Student License  
Downloads  
Resellers  
Cancel subscription  
Contact Us



[English](#)

[Portuguese](#)

[日本語](#)

[中文](#)

