

## Apache Log4j library security vulnerability and M-Files

Version 5

Last updated: 16/12/2021, 11:45 AM EET

Dear Customer,

We wish to inform you that in response to the published vulnerabilities on Apache Log4j (CVE-2021-44228 and CVE-2021-45046) M-Files Security team has performed a rigorous review to identify any potential exposure and risks arising from the vulnerability.

M-Files core product relies on programming languages other than Java, and thus we have not as of now identified use of vulnerable log4j library within M-Files Server / Desktop / Classic Web / VNEXT / Mobile services.

For Smart Search, IDOL and other services, we have updated all components that have come to our attention where the risk of exposure to the vulnerability could not be ruled out.

For Hubshare Cloud product we have performed all critical updates for components that have come to our attention where the risk of exposure to the vulnerability could not be ruled out. For Hubshare on-premises installations a patch routine causing minimal downtime has been released. M-Files Security team shall continue investigations and we shall keep you informed should we have additional information to share.

Best regards,

M-Files Security

### Change log:

Version 1	First notification
Version 2	Content on Hubshare added
Version 3	Content on Smart Search added
Version 4	Content on IDOL added
Version 5	Response updated over CVE-2021-45046