Subject	**VisualSoft and Apache Log4**
Date	**26 January 2022**
Author	**Bill Parker-Jervis, Technical Manager - VisualSoft**

1 INTRODUCTION

In late 2021 news started to circulate about a security vulnerability in a widely used Java logging library, potentially putting the users of many software applications at risk. For details of the threat, please see https://www.ncsc.gov.uk/information/log4j-vulnerability-what-everyone-needs-to-know. This memo explains why users of the VisualSoft Suite and its associated tools and applications, and any users of NAS drives supplied by VisualSoft should not need to worry about this vulnerability in the context of VisualSoft applications and systems.

2 VISUALSOFT SUITE AND VISUALREVIEW SOFTWARE

The Log4j vulnerability has no impact on any VisualSoft applications or systems (current or legacy) because we do not use Java, and have never done so in any release of any of our applications.

Log4j and the associated vulnerability is specific to the use of Java code for logging (typically things such as audit type logs). In the VisualSoft Suite applications we do not use Java for audit logging or for any other purpose.

For the avoidance of any doubt: In one rare circumstance we do use Java Script (which is not the same thing as Java code). Java Script is deployed if users choose the “web report” option when generating a VisualWorks Report. i.e. instead of exporting data for use in VisualReview they may choose to export data for use in a web browser. If so, some Java Script is included with the generated web pages. That Java Script has no logging capability and so on multiple counts (not being Java, not logging, and not using Log4j) it is not relevant in the context of the Log4j vulnerability.

Applications in the VisualSoft Suite include VisualDVR, VisualOverlay, Visual3D-Inspector, VisualData Logger, VisualArchive, VisualEdit (all editions), VisualEventLogger, Admin Panel, and associated add-ons and tools. VisualReview and VisualReview Professional use the same underlying code as applications in the VisualSoft Suite, and so the explanations given above apply also to both editions of VisualReview.

3 NAS AND OTHER STORAGE DEVICES

NAS drives from Avante Digital (AV-STOR), or from Synology, as supplied by VisualSoft are not affected by any Log4j vulnerability.

Users of other NAS or SAN devices should check with the relevant manufacturer and should pay particular attention to any 3rd Party applications installed directly on their device for tasks such as automated synchronisation.