Gather Workload Data

DESCRIPTION

This agent procedures helps detect if the target machine is a victim of Log4j vulnerability.
Procedure folder consists of an exe file and a shell file.

Please note that this procedure only helps to detect the vulnerability but does not include the mitigation steps.

If vulnerability is detected the information on the vulnerability is saved as TXT- file named *{AgentID}*- *{DateTime}***.txt** on the VSA server in the Kaseya folder under UserProfiles\Log4jDetect.

INSTALL INSTRUCTIONS

1. Extract the files from the attached zip file.

2. Import the XML into the agent procedure module: https://helpdesk.kaseya.com/hc/en-gb/articles/229012068.

3. Execute the procedure on a target machine.

DISCLAIMER

Kaseya has used the Open Source LunaSec Detection Tool (https://www.lunasec.io/docs/blog/log4j-zero-day-mitigation-guide/) to assist with the detection of the Log4J vulnerability, but due to the environmental variables and in keeping with best security practices, a clean result cannot guarantee protection from compromise. Kaseya recommends use of this script in conjunction with a layered organizational defensive strategy for most complete protection.