# DESCRIPTION

This agent procedures helps detect if the target machine is a victim of Log4j vulnerability.

Procedure folder consists of an exe file, a shell file and a PowerShell file.

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

# Install instructions

1. Extract the files from the attached zip file

2. Upload the PowerShell file **FindLog4j.ps1** and LunaSec utilities (log4shell.exe, log4shell) to the Shared Files/ directory of the Managed Files folder: <https://helpdesk.kaseya.com/hc/en-gb/articles/360017878358>

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

4. Execute desired agent procedure on the target machine.