DESCRIPTION

This procedure will check exchange servers for vulnerabilities identified by Microsoft in the following article: https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/#scan-log

The procedure checks for potential [CVE-2021-26855], [CVE-2021-26857], [CVE-2021-26858], and [CVE-2021-27065] vulnerabilities and reports it to the script log. If a potential vulnerability is identified, an alarm is generated for that agent.

Specific logs that are triggered as being evidentiary of vulnerability are uploaded to the GetFile page per agent for further review.

Note: Kaseya has used and slightly modified Microsoft Security Tests made for these vulnerabilities (https://github.com/microsoft/CSS-Exchange/tree/main/Security) in the creation, but due to the polymorphic nature of advanced threats, a clean result does not guarantee a protection from compromise. Kaseya recommends use of this script in conjunction with a layered organizational defensive strategy for most complete protection.

INSTALL INSTRUCTIONS

1. Extract the files from the attached zip file.

2. Upload the Power Shell file 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 the procedure on a target machine.