MOTOROLA SOLUTIONS

DOCUMENT NUMBER: MTN-0023B-23-NA
APC: 877
ISSUE DATE: Apr-2023
EXPIRATION DATE: 30-Apr-2024
Bulletin Type: Informational Only

Motorola Solutions Technical Notification (MTN)

TITLE: Update procedure for CSMS Host-Based to ePO 5.10.0 update 14 containing log4j version 2.17.1 and procedure to fix events forwarding issue.

TECHNOLOGY: ASTRO P25 - Host-Based CSMS

SYMPTOMS:
Systems running CSMS Host-Based with McAfee ePO 5.10.0 Update 7, 9 and 10 contain an outdated log4j version.

NOTICE: This MTN is for **CSMS Host-Based** systems ONLY.

Use Case 1 - DO NOT APPLY: Do not apply this MTN to any system with Standard CSMS. There is a separate MTN to address Standard CSMS systems (follow MTN-0223-22-NA or later).

Use Case 2 - OPTIONAL: Systems running **CSMS Host-Based** with McAfee ePO 5.10.0 update 10, update 9 or update 7 contain a **non-vulnerable** version of log4j. For systems that have an internal mandate to remove all instances of log4j 1.x, this MTN removes the non-vulnerable log4j 1.x and replaces it with version 2.17.1.

Use Case 3 - REQUIRED: Systems running **CSMS Host-Based** that purchase SUS McAfee updates. Systems running **CSMS Host-Based** with McAfee ePO 5.10.0 update 12. **2022.1** systems running **Host-Based CSMS**.

MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED:
A2019.2/A2020.1/A2020.HS/A2021.1/A2022.1/A2022.HS - **CSMS Host-Based**

- McAfee ePO 5.10.0 Update 12, 10, 9, and 7

SEVERITY RECOMMENDATION: **Medium / Operational** - Schedule to implement

ROOT CAUSE: Third-party application defect

DEFINITIVE TEST:
To determine if the CSMS is Standard or Host-Based:

1. Login to CSMS
2. Launch Powershell as an Administrator
3. Type the following command:
    a. (Get-ItemProperty -Path HKLM:\SOFTWARE\MotorolaSolutions\).'OVF Version'
4. If the Version returned begins with CSMS-Astro then this is a CSMS Standard system. If the Version returned begins with CSMS-HB then this is a CSMS Host-Based system.

To determine the current ePO version:

1. Login to CSMS
2. ***Launch McAfee ePolicy Orchestrator 5.10.0 Console*** from CSMS Desktop
3. Login to McAfee ePolicy Orchestrator with admin credentials

DOCUMENT NUMBER: MTN-0023B-23-NA
APC: 877
ISSUE DATE: Apr-2023
EXPIRATION DATE: 30-Apr-2024
Bulletin Type: Informational Only

4. Launch the ***Main Menu***, click the 3 horizontal bars
5. Select ***Server Settings*** under **Configuration**
6. Under **Setting Categories**, select ***Server Information***
7. In the **Server Information** section you will look for **Version** which is the ePO version installed as well as **Update Installed** which is the Update to ePO that is installed.
8. If the **Update Installed** is **Update 12**, you only need to run **Procedures 4, 5, 6, 7, 8 and 9** (below).
9. Otherwise, if your version matches any other listed above (update 7, 9 or 10), perform **RESOLUTIONS AND REPAIR PROCEDURES** Section below.

NOTE: If you already applied the first version of this MTN (means your current update version of McAfee ePO 5.10.0 is 14), there is no need to apply complete procedure, you only need to run **Procedure 9** (below).
NOTE 1: This version contains some minor clarification points based on customers input. Changes compared to the previous revision of this MTN are highlighted in yellow.

WORKAROUNDS:
None

CORRECTIVE ACTIONS:
Follow the **RESOLUTIONS AND REPAIR PROCEDURES** Section below.

RESOLUTIONS AND REPAIR PROCEDURES:

1. Run ***Procedure 1: Import Product Compatibility List - Update 12*** (below)
2. Run ***Procedure 2: Import Extensions - Update 12*** (below)
3. Run ***Procedure 3: Upgrade to ePO Update 12*** (below)
4. Run ***Procedure 4: Import Product Compatibility List - Update 14*** (below)
5. Run ***Procedure 5: Import Extensions - Update 14*** (below)
6. Run ***Procedure 6: Upgrade to ePO Update 14*** (below)
7. Run ***Procedure 7: Import Automatic Response*** (below)
8. Run ***Procedure 8: Import CSMS Policies*** (below)
9. Run ***Procedure 9: Remove Outdated Update Folders*** (below)
10. Repeat this for CSMS02 if the system is DSR (Dynamic System Resilience)

To obtain software:
1) Initiate a software request case through Motorola Solutions, Inc. Centralized Managed Support Operations (CMSO) at 800-MSI-HELP (800-674-4357) or 302-444-9800
2) Await confirmation email from Motorola Solutions Software Factory (MSSF) with instructions
3) Complete the Motorola Solutions Software Factory Software Order Form:
   a) Reference **MTN-0023B-23-NA** in the 'Reason for Software/Hardware Change' section of the software order form.
   b) List the part number (**KC #** as listed under "PARTS REQUIRED (HARDWARE/SOFTWARE)" below) in the 'Part # or Version #' section of the software order form.

Email completed Software Order Form to MSSF for processing

TIME TO IMPLEMENT/SYSTEM IMPACT:
Medium - time consuming but no loss of functionalities
Estimated time to implement - per machine: 1 Hour

MOTOROLA SOLUTIONS

DOCUMENT NUMBER: MTN-0023B-23-NA
APC: 877
ISSUE DATE: Apr-2023
EXPIRATION DATE: 30-Apr-2024
Bulletin Type: Informational Only

PARTS REQUIRED (HARDWARE/SOFTWARE):
A2019.2/A2020.1/A2020.HS/A2021.1/A2022.1/A2022.HS

- CSMS Configuration Disk - R07.01.18 or later
  - KC877V0C4000000116 or later
- CSMS Supplementary Disk - R08.04.31 or later
  - KC877C085000000112 or later

ADDITIONAL INFORMATION: None

REFERENCE THE FOLLOWING DOCUMENTS/PROCESSES FOR INSTALLATION PROCEDURES:
GCD Manuals:

1. MN007181A01 - Core Security Management Server Feature Guide

Additional Installation Procedures:
Procedure 1: Import Product Compatibility List - Update 12

Time to Perform:	20 min
Before You Begin:	Obtain CSMS Configuration Media version R07.01.18 or newer. Obtain the ePO console admin credentials to login to the ePO console.
Notes:	Perform this procedure on the Core Security Management Server (CSMS) in the primary core and the backup core if CSMS in the backup core exists.
Procedure 1.1:	Import Product Compatibility List - Update 12
1.	Mount the CSMS Configuration Media to the CSMS VM.
2.	Log on to the CSMS VM with administrative credentials
3.	***Launch McAfee ePolicy Orchestrator 5.10.0 Console*** from CSMS Desktop
4.	Login to McAfee ePolicy Orchestrator with admin credentials
5.	Launch the ***Main Menu***, click the 3 horizontal bars
6.	Select ***Server Settings*** under the **Configuration** column
7.	Scroll down and select **Product Compatibility List**
8.	Click ***Edit***
9.	Select **Disabled**
10.	Click ***Browse***
11.	Navigate to **<DVD Drive>/ePO_Update/ePO_5.10.0_Update_12/STD_Extensions/ProductCompatibilityList.xml**
12.	Click ***Open***

13.	Click **Save**
14.	Come back to the section **RESOLUTIONS AND REPAIR PROCEDURES:** of this MTN and continue the next steps accordingly.

Procedure 2: Import Extensions - Update 12

Time to Perform:	20 min
Before You Begin:	Obtain CSMS Configuration Media version R07.01.18 or newer. Obtain the ePO console admin credentials to login to the ePO console.
Notes:	Perform this procedure on the Core Security Management Server (CSMS) in the primary core and the backup core if CSMS in the backup core exists.
Procedure 2.1:	Import Extensions - Update 12
1.	Mount the CSMS Configuration Media to the CSMS VM.
2.	Log on to the CSMS VM with administrative credentials
3.	***Launch McAfee ePolicy Orchestrator 5.10.0 Console*** from CSMS Desktop
4.	Login to McAfee ePolicy Orchestrator with admin credentials
5.	Launch the ***Main Menu***, click the 3 horizontal bars
6.	Select ***Extensions*** under the **Software** column
7.	Click ***Install Extension***
8.	Click ***Browse***
9.	Navigate to **<DVD Drive>/ePO_Update/ePO_5.10.0_Update_12/STD_Extensions/Endpoint_Security_Platform_10.7.0.1076_Extension.zip**
10.	Click ***Open***
11.	Click ***OK***
12.	Click ***OK*** ***Note: If a newer version of the extension is already installed, just click Cancel***
13.	Repeat Steps 7 through 12 for the following packages: **- EPOAGENTMETA.zip** **- Threat_Prevention_10.7.0.1248_Extension.zip**

	- UpgradeAssistant_2.11.0.70.zip **- Web_Control_10.7.0.1162_Extension.zip** **NOTE: If upon importing the extensions you get a note that says the extension version is lower than what is currently installed you can skip that extension and move on to the others.**
14.	Click ***Install Extension***
15.	Click ***Browse***
16.	Navigate to **<DVD Drive>/ePO_Update/ePO_5.10.0_Update_12/HB_Extensions/Firewall_10.7.0.1116_Extension.zip**
17.	Click ***Open***
18.	Click ***OK***
19.	Click ***OK*** ***Note: If a newer version of the extension is already installed, just click Cancel***
20.	Repeat Steps 14 through 19 for the following packages: **- DLP_Mgmt_11.9_Package.zip** **- RSD_EXTENSION_5.0.6_151.zip** **- Solidcore_epo_extn_8.3.4.124.zip** **- PAPackage.zip** **NOTE: If upon importing the extensions you get a note that says the extension is older then what is currently installed you can skip that extension and move on to the others.**
21.	Come back to the section **RESOLUTIONS AND REPAIR PROCEDURES:** of this MTN and continue the next steps accordingly.

Procedure 3: Upgrade to ePO Update 12

Time to Perform:	10 min
Before You Begin:	Obtain CSMS Configuration Media version R07.01.18 or newer. Obtain the eposql2 DB credentials for the upgrade of ePO.
Notes:	Perform this procedure on the Core Security Management Server (CSMS) in the primary core and the backup core if CSMS in the backup core exists.
Procedure 3.1:	Upgrade to ePO Update 12
1.	Mount the CSMS Configuration Media to the CSMS VM.

2.	Log on to the CSMS VM with administrative credentials
3.	**Open File Explorer**
4.	Navigate to **<DVD Drive>:/ePO_Update/ePO_5.10.0_Update_12**
5.	Copy **ePO_5.10.0_Update_12.zip** to the **Desktop**
6.	Right-click on the ePO_5.10.0_Update_12.zip on the Desktop and select **Extract All**
7.	Make sure **Show extracted files when complete** is checked
8.	Select **Extract**
9.	In the folder that opens after extraction, double-click on **ePOUpdater.exe**
10.	Enter the **Password** for eposql2
11.	Click the **I accept the license agreement** checkbox, then select **Continue**
12.	Select **Continue**
13.	Click **OK**
14.	Click **Finish**
15.	Come back to the section **RESOLUTIONS AND REPAIR PROCEDURES:** of this MTN and continue the next steps accordingly.

Procedure 4: Import Product Compatibility List - Update 14

Time to Perform:	20 min
Before You Begin:	Obtain CSMS Configuration Media version R07.01.18 or newer. Obtain the ePO console admin credentials to login to the ePO console.
Notes:	Perform this procedure on the Core Security Management Server (CSMS) in the primary core and the backup core if CSMS in the backup core exists.
Procedure 4.1:	Import Product Compatibility List - Update 14
1.	Mount the CSMS Configuration Media to the CSMS VM.
2.	Log on to the CSMS VM with administrative credentials
3.	***Launch McAfee ePolicy Orchestrator 5.10.0 Console*** from CSMS Desktop
4.	Login to McAfee ePolicy Orchestrator with admin credentials
5.	Launch the ***Main Menu***, click the 3 horizontal bars

6.	Select ***Server Settings*** under the **Configuration** column
7.	Scroll down and select **Product Compatibility List**
8.	Click ***Edit***
9.	Select **Disabled**
10.	Click ***Browse***
11.	Navigate to **<DVD Drive>/ePO_Update/ePO_5.10.0_Update_14/STD_Extensions/ProductCompatibilityList.xml**
12.	Click ***Open***
13.	Click **Save**
14.	Come back to the section **RESOLUTIONS AND REPAIR PROCEDURES:** of this MTN and continue the next steps accordingly.

Procedure 5: Import Extensions - Update 14

Time to Perform:	20 min
Before You Begin:	Obtain CSMS Configuration Media version R07.01.18 or newer. Obtain the ePO console admin credentials to login to the ePO console.
Notes:	Perform this procedure on the Core Security Management Server (CSMS) in the primary core and the backup core if CSMS in the backup core exists.
Procedure 5.1:	Import Extensions - Update 14

1.	Mount the CSMS Configuration Media to the CSMS VM.
2.	Log on to the CSMS VM with administrative credentials
3.	***Launch McAfee ePolicy Orchestrator 5.10.0 Console*** from CSMS Desktop
4.	Login to McAfee ePolicy Orchestrator with admin credentials
5.	Launch the ***Main Menu***, click the 3 horizontal bars
6.	Select ***Extensions*** under the **Software** column
7.	Click ***Install Extension***
8.	Click ***Browse***
9.	Navigate to **<DVD Drive>/ePO_Update/ePO_5.10.0_Update_14/HB_Extensions/PAPackage.zip**
10.	Click ***Open***

11.	Click ***OK***
12.	Click ***OK*** ***Note: If a newer version of the extension is already installed, just click Cancel***
13.	Repeat Steps 7 through 12 for the following packages: **- RSD_EXTENSION_5.0.6.172.zip** **- DLP_Mgmt_11.9_signed.zip** **NOTE: If upon importing the extensions you get a note that says the extension version is lower than what is currently installed you can skip that extension and move on to the others.**
14.	Come back to the section **RESOLUTIONS AND REPAIR PROCEDURES:** of this MTN and continue the next steps accordingly.

Procedure 6: Upgrade to ePO Update 14

Time to Perform:	10 min
Before You Begin:	Obtain CSMS Configuration Media version R07.01.18 or newer. Obtain the eposql2 DB credentials for the upgrade of ePO.
Notes:	Perform this procedure on the Core Security Management Server (CSMS) in the primary core and the backup core if CSMS in the backup core exists.
Procedure 6.1:	Upgrade to ePO Update 14
1.	Mount the CSMS Configuration Media to the CSMS VM.
2.	Log on to the CSMS VM with administrative credentials
3.	**Open File Explorer**
4.	Navigate to **<DVD Drive>:/ePO_Update/ePO_5.10.0_Update_14**
5.	Copy **ePO_5.10.0_Update_14.zip** to the **Desktop**
6.	Right-click on the ePO_5.10.0_Update_14.zip on the Desktop and select **Extract All**
7.	Make sure **Show extracted files when complete** is checked
8.	Select **Extract**
9.	In the folder that opens after extraction, double-click on **ePOUpdater.exe**
10.	Enter the **Password** for eposql2

11.	Click the **I accept the license agreement** checkbox, then select **Continue**
12.	Select **Continue**
13.	Click **OK**
14.	Click **Finish**
15.	Come back to the section **RESOLUTIONS AND REPAIR PROCEDURES:** of this MTN and continue the next steps accordingly.

Procedure 7: Import Automatic Response

Time to Perform:	10 min
Before You Begin:	Obtain the ePO console admin credentials to login to the ePO console.
Notes:	Perform this procedure on the Core Security Management Server (CSMS) in the primary core and the backup core if CSMS in the backup core exists. If this procedure has already been run there is no need to run again. You can verify this by checking for the following Automatic Responses: "MSI: Send ePO Malware events to Windows event log 1027" "MSI: Send ePO Malware events to Windows event log 1278"
Procedure 7.1:	Import Automatic Response

1.	Mount the CSMS Configuration Media to the CSMS VM.
2.	Log on to the CSMS VM with administrative credentials
3.	***Launch McAfee ePolicy Orchestrator 5.10.0 Console*** from CSMS Desktop
4.	Login to McAfee ePolicy Orchestrator with admin credentials
5.	Launch the ***Main Menu***, click the 3 horizontal bars
6.	Select **Automatic Responses** under **Automation**
7.	Click **Import Responses**
8.	Click **Browse**
9.	Navigate to **<DVD drive>:/2020.1/XML/Base/Automatic Response**
10.	Select **Automatic_Responses_new.xml**
11.	Click **Open**
12.	Click **OK**

13.	There are two **Automatic Responses** being imported (shown in the left column).
14.	For each **Automatic Response** being imported
15.	In the right window pane click the box for **Enable response**
18.	Click **OK**
19.	Click **OK**
20.	Come back to the section **RESOLUTIONS AND REPAIR PROCEDURES:** of this MTN and continue the next steps accordingly.

Procedure 8: Import CSMS Policies

Time to Perform:	10 min
Before You Begin:	Obtain the ePO console admin credentials to login to the ePO console.
Notes:	Perform this procedure on the Core Security Management Server (CSMS) in the primary core and the backup core if CSMS in the backup core exists. **Ensure that:** **• Your CSMS contains ePO 5.10. NOTE: The procedure does not work on ePO 5.9.** **• The version of your CSMS is R08.04.26 or later. See *Verifying CSMS and Windows Supplementary Versions* in the manual below. If a proper version is not installed, see Installing *CSMS Supplementary Version* in the manual below. Obtain the latest version of the CSMS Config media listed in the section PARTS REQUIRED above .**
Procedure 8.1:	Import CSMS Policies

1.	Mount the CSMS Configuration Media to the CSMS VM.
2.	Log on to the CSMS VM with administrative credentials
3.	Right-click **Start** and select **Search**
4.	Type ***powershell***
5.	Right-click **Windows PowerShell**, and select **Run as administrator**
6.	If the **User Account Control** windows appears, click **Yes**
7.	Change to scripts directory by typing: *cd C:\Program Files\Motorola\AstroCSMS\McAfeeServer\scripts*
8.	Import the new policies into CSMS by entering the following command: ***.\ImportEpoPolicies.ps1***
9.	Come back to the section **RESOLUTIONS AND REPAIR PROCEDURES:** of this MTN and continue the next steps accordingly.

DOCUMENT NUMBER: MTN-0023B-23-NA
APC: 877
ISSUE DATE: Apr-2023
EXPIRATION DATE: 30-Apr-2024
Bulletin Type: Informational Only

Procedure 9: Remove Outdated Update Folders

Time to Perform:	10 min
Before You Begin:	Obtain the ePO console admin credentials to login to the ePO console.
Notes:	Perform this procedure on the Core Security Management Server (CSMS) in the primary core and the backup core if CSMS in the backup core exists.
Procedure 9.1:	Remove Outdated Update Folders
1.	Log on to the CSMS VM with administrative credentials
2.	Right-click **Start** and select **Search**
3.	Type ***powershell***
4.	Right-click **Windows PowerShell**, and select **Run as administrator**
5.	If the **User Account Control** windows appears, click **Yes**
6.	Enter the following command: ***remove-item 'C:\Program Files (x86)\McAfee\ePolicy Orchestrator\updates*CU*' -Recurse -Force***
7.	Come back to the section **RESOLUTIONS AND REPAIR PROCEDURES:** of this MTN and continue the next steps accordingly.

WHEN TO APPLY RESOLUTION:
Immediately _X_

LABOR ALLOWANCE:
This is an informational bulletin. No labor warranty is implied, intended or authorized for U.S. Domestic Partners/Customers. Other regions should follow their own standard procedures.

If, after attempting to perform the solution steps, you are having issues with the resolution in the MTN then please contact your MSI Technical support center.
https://www.motorolasolutions.com/en_us/support.html

SW ORDER FORM IS AVAILABLE UNDER THE LINK:
http://www.motorolasolutions.com/content/dam/msi/docs/robots/motorola-technical-notification/SW_order_form.pdf