MOTOROLA SOLUTIONS

DOCUMENT NUMBER: MTN-0006-20-NA
APC: 877
ISSUE DATE: 01-2020
EXPIRATION DATE: 31-0-2021
Bulletin Type: Informational Only

Motorola Solutions Technical Notification (MTN)

TITLE: Microsoft DISM.exe and Spawned Processes are blocked by McAfee Access Protection

TECHNOLOGY: ASTRO® 25 Infrastructure

SYMPTOMS:

- NPS or Server Manager can't be run on Domain Controllers
- DC services such as RADIUS authentication and Active Directory replication may not work properly
- Local backups fail on CSMS(Core Security Management Server)

MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED:

Earlier builds of CSMS have missing exclusions preventing Microsoft's DISM.exe from executing correctly on Windows devices. These are the builds of CSMS that are known to be missing the necessary exclusions AND there are documented cases reporting issues in customer environments:

- A2019.2
  - CSMS versions:
    - 19.02.00.09

These are the builds of CSMS that are known to be missing these exclusions BUT there have been no documented cases reporting issues in customer environments yet:

- A7.17.3 - A7.18
  - CSMS versions:
    - 07.17.00-17
    - 07.18.00-17

How to check CSMS version with PowerShell (64 bit version only, do not use "Windows PowerShell (x86)"):

```
(Get-ItemProperty -Path HKLM:\SOFTWARE\MotorolaSolutions).'OVF Version'
```

SEVERITY RECOMMENDATION:

Medium / Operational - Schedule to implement

ROOT CAUSE / DEFINITIVE TEST:

CSMS is one of the versions detailed in the *MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED* section AND NPS or Server Manager can't run on DCs without applying a workaround OR backups on CSMS are failing.

WORKAROUNDS AND CORRECTIVE ACTIONS:

Prerequisites:

- Obtain administrator credentials for CSMS and McAfee's ePO application
- Obtain the KC877V0C4000<REL6>.iso (a.k.a *CSMS_Config_Media*) for your ASTRO release
  where <REL6> is the last 6 digits representing the ASTRO release

Procedure:

Note: Perform this procedure for CSMS01 (and CSMS02, if it's a DSR system). This procedure is written for McAfee ePO v5.10

1. Create a folder on the CSMS Desktop called *CSMS_Config*
2. Copy the *CSMS_Config_Media.iso* contents to the *CSMS_Config* folder on the CSMS Desktop
    a. Result: Two folders are placed into the *CSMS_Config* folder: XML and XML_HB
3. Double click on the **Launch McAfee ePolicy Orchestrator x.x.x Console** icon on the CSMS desktop
4. Log on to the ePO console with administrator privileges
5. In the top bar, click **Policy Catalog**
6. WARNING: You are about to import new **Access Protection** and **Exploit Prevention** policies. If customization has been performed on top of these policy categories, they are about to be overwritten. If there is customization in the policies, take note of the custom policy settings so they can be reintroduced after the import is complete.
7. Towards the right hand side, below the McAfee toolbar, find the **New Policy** button. Click the dropdown next to **New Policy** and click **Import**.
8. Click **Browse** and navigate to **Desktop > CSMS_Config > XML > Base > ENS Threat Protection** and select the ***Policies_For_Endpoint_Security_Threat_Prevention*** file and click **Open**
9. Click **OK**
10. Unselect all policies by unchecking the top-most checkbox (immediately to the left of *Product*)
11. Re-check the checkboxes for those policies of category **Access Protection** and **Exploit Prevention** (you may have to scroll down to see them)
    a. Note: You can ignore the "Note: Importing policies marked with red will overwrite the existing identically named policy and assume their assignments." warning. This is what we're trying to do.
12. Click **OK** at the bottom right of the screen. It will take some time to import, the screen may appear frozen, just let it finish before clicking again.
13. Verify the import was successful by navigating to **Policy Catalog**, clicking **Endpoint Security Threat Prevention** in the left pane, expanding **Access Protection** in the right pane, clicking **Edit** for the ***MSI_STIG_Compliant AP Windows***
14. Click **Show Advanced**
15. In the **Exclusions** section, ensure exclusions named ***Microsoft product by signature <1-7>*** are present. If it is present, the configuration change was successful.
16. Click **Cancel** at the bottom right of the screen.
17. In the top bar, click **System Tree**
18. From **Preset** dropdown select **This Group and All Subgroups**
19. In the **Custom** dropdown select **Windows** if available, otherwise click **Add…**
    a. Follow these substeps only if you clicked **Add…** in the previous step
    b. In the **Available Properties** (left) pane, scroll down and click **OS Type**
    c. In the right pane, for the ***Value*** click **Windows 10**
    d. Click the **+** to the right of the ***Value*** field
    e. For the second ***Value*** click **Windows Server 2012 R2**
    f. Click the **+** to the right of the second ***Value*** field
    g. For the third ***Value*** click **Windows Server 2016**
    h. Click **Update Filter** on the bottom right of the screen
    i. In the **Custom** dropdown, click the dropdown, and then hover over the dropdown for the ***(unsaved)*** entry, click **Save**
    j. Enter the name **Windows**
    k. Click **OK**
20. Select the checkboxes for all Windows devices
21. Click **Wake Up Agents**
22. Select the checkbox for "Force complete policy and task update"
23. Click **OK** and take note of the time
24. Delay 2 minutes, then refresh the system tree page
    Result: All Windows devices in system tree show last communication after the noted time, the new policies have been applied to the selected Windows devices and the new configuration has been pushed to the Windows devices.
25. You can now exit the ePO application and log off of the CSMS.
26. If the system is DSR, repeat this procedure on the backup CSMS.

RESOLUTIONS AND REPAIR PROCEDURES:

Apply this MTN (procedure detailed in the *WORKAROUNDS AND CORRECTIVE ACTIONS* section) to those fielded ASTRO® 25 systems (A2019.2) that are affected as described in the *MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED* section.

PARTS REQUIRED (HARDWARE/SOFTWARE):

A2019.2 CSMS Configuration Media (KC877V0C4000000102)
A7.18 CSMS Configuration Media (KC877V0C4000000102)
A7.17.3 CSMS Configuration Media (KC877V0C4000000102)

ADDITIONAL INFORMATION:

This procedure will have to be redone if the CSMS is reinstalled and is one of the versions as detailed in the *MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED* section. If restoring CSMS from BAR backups taken after this configuration change, you won't have to reapply this MTN as the configuration is saved in the backup. If installing a newer version of CSMS, this configuration change is already included in the default CSMS build.

REFERENCE THE FOLLOWING DOCUMENTS/PROCESSES FOR INSTALLATION PROCEDURES:

For reference material, the following full GCD manuals can be referred to:

- A2019.2 Core Security Management Server Feature Guide (MN005942A01)

WHEN TO APPLY RESOLUTION:

After reboot __
After (re)installation _x_
After upgrade __
After power cycle __
After database restoration __
After failure __
On FRU replacement __
During maintenance __
Immediately __
As instructed _x_
Information only __

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.

For assistance with this bulletin please contact your MSI Technical support center
https://www.motorolasolutions.com/en_us/support.html

MOTOROLA SOLUTIONS

Upgrade Operations Software Team

Software Order Form
Phone Number: (800) 221-7144

SECTION 1: General Information

NOTE: PRICE QUOTES GIVEN BY UOST ARE VALID FOR ONLY 90 DAYS

Date		Case Number	
System ID		Site ID	
System Name		Site Name	
Customer Name			
Form Completed by		Field Contact	
Organization		Organization	
Phone Number		Phone Number	
Pager Number		Pager Number	
Fax Number		Fax Number	

SECTION 2: Order Information

Product Type: _____ Serial Number _____

Reason for Software / Hardware Change: _____
Downgrade? If so, list current and target releases. _____

Software / Hardware Description: _____

Part # or Version # _____ Quantity _____

Date Required _____

SECTION 3: Shipping / Billing Information

Ship To:		Bill To:	
Email:			
Attn:		Attn:	
Phone:		Phone:	

Customer Billing		Internal Billing	
P.O. #:		PROJECT #:	
CUST #:		FSB #:	
TAG #:		DEPT #:	
		APC #:	

MOTOROLA SOLUTIONS

Software Order Form

Upgrade Operations Software Team

Phone Number: (800) 221-7144

° This form has been sent to you because you have requested an order from the Upgrade Operations Software Team.

° Please fill out the order form and email back to the Upgrade Operations Software Team

° If desired, please provide your email address on the order form and we will provide a tracking number when your order ships for your convenience.

° Orders will normally be processed in 3-5 business days once all information has been received.

° If additional space is required for software information, please use the optional addendum on page 3 below in addition to the original order form. This form is for use with large orders with multiple part numbers.

NOTE:

1) If this in an SSA CUSTOMER please order via Motorola factory order.
2) Limited Liability is Implied to the maximum of order amount.
3) Price quotes provided by UOST are valid for 90 days

Thank you and have a good day!

Supplemental Order Information Addendum

(Optional)

Software Description _____

Part# or Version # _____

Quantity: _____

Software Description _____

Part# or Version # _____

Quantity: _____

Software Description _____

Part# or Version # _____

Quantity: _____

Software Description _____

Part# or Version # _____

Quantity: _____

Software Description _____

Part# or Version # _____

Quantity: _____

Software Description _____

Part# or Version # _____

Quantity: _____