MOTOROLA SOLUTIONS

DOCUMENT NUMBER: MTN-0055-17-NA
APC: 708
ISSUE DATE: 04-2017
EXPIRATION DATE: 30-04-2018
Bulletin Type: Informational Only

Motorola Solutions Technical Notification (MTN)

TITLE: Radio Control Manager (RCM) Web Interface Inaccessible & IVD Voice and Data Becomes Unreliable

TECHNOLOGY:
ASTRO 7.16 Radio Control Manager (RCM)
ASTRO 7.13, 7.14, 7.15, and 7.16 IVD Voice and Data

SYMPTOMS:
ASTRO 7.16 Radio Control Manager (RCM) Web Interface Inaccessible
ASTRO 7.13, 7.14, 7.15, and 7.16 IVD Voice and Data Unreliable Approximately 15 Minutes Starting 10PM Daily

MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED:
ASTRO 7.13, 7.14, 7.15, and 7.16 with Motopatch for McAfee 2016.Q4, 2016.Q4.1, or 2016.Q4.2 Applied

SEVERITY RECOMMENDATION:
High / Safety - Perform Immediately

ROOT CAUSE / DEFINITIVE TEST:

Root Cause:
McAfee VirusScan Enterprise (VSE) On-Access Scanner was enabled on Red Hat Enterprise Linux (RHEL) 6 devices by Motopatch for McAfee 2016.Q4 and 2016.Q4.1. This results in an inability to access the ASTRO 7.16 Radio Control Manager (RCM) web interface and may result in other performance impacts on ASTRO 7.13, 7.14, 7.15, and 7.16. In addition, a QuickScan was scheduled to run daily at 10PM on ZC01, ZC02, and PDG_IVD. This results in IVD voice and data potentially becoming unreliable for approximately 15 minutes on ASTRO 7.13, 7.14, 7.15, and 7.16 systems, while the scan is running.

Definitive Test:
If Motopatch for McAfee 2016.Q4, 2016.Q4.1, or 2016.Q4.2 have been applied, the McAfee ePolicy Orchestrator (ePO) application on the Central Security Management Server (CSMS) will possess the policy and client tasks shown in the procedure contained in the following workarounds and corrective actions section.

WORKAROUNDS AND CORRECTIVE ACTIONS:
This procedure will disable Virus Scan Enterprise (VSE) On-Access Scanner on Red Hat Enterprise Linux (RHEL) 6 devices and will disable the QuickScan scheduled to run daily at 10PM on ZC01, ZC02, and PDG_IVD.

Policy Catalog and Assignment Amendment:

1. Log into the CSMS with domain administrator account.
2. From the desktop, open the ePO 5.1.3 Console shortcut.
3. Log into the ePO application with an account granted global administrator privileges. (Motorola default is csmsadmin)
4. From the top left hand section, select Menu > Policy Catalog.

Result: The Policy Catalog page appears.

5. Select the drop down arrow for the Product filter, and choose VirusScan Enterprise for Linux 1.9.2 / 2.0.3.

Result: The Policy Catalog page refreshes, displaying policies for VirusScan for Linux 1.9.2 / 2.0.3

6. Under the Name column, select by clicking, the policy named *MSI_Disable_On-Access_scan_VSEL_1.9.2.*

Result: The page will refresh with the General tab displayed.

7. Under the General Tab, uncheck the box, *Enable On-access scanning...*

8. Click Save on the bottom right hand side of the page.

Result: The page will refresh, and return back to the Policy Catalog Page.

9. Under the Name column, select by clicking, the policy named *MSI_Linux_Default_STIG_Compliant_VSE_1.9.2.*

Result: The page will refresh with the General tab displayed.

10. Under the General Tab, uncheck the box, *Enable On-access scanning...*
11. Click Save on the bottom right hand side of the page.

Result: The page will refresh, and return back to the Policy Catalog Page

12. From the top left hand section, select Menu > Policy Assignments.
13. On the left hand rail, ensure that My Organization is highlighted in yellow.
14. From the Product drop down, click the arrow to select VirusScan Enterprise for Linux 1.9.2 / 2.0.3.
15. Under the Category column, identify the On-Access Policy row, and select Edit Assignment under the Actions column.
16. Ensure that the following settings are configured:
17. If not already set, set Break inheritance and assign the policy and settings below.
18. If not already set, set Assigned Policy to “MSI_Disable_On-Access scan VSE 1.9.2”
19. Lock policy inheritance is “Unlocked”
20. After you have confirmed these settings, click Save at the bottom of the page.
21. From the top left hand section, select Menu > Policy Assignment Rules.
22. Find the two Policy Assignment Rules labeled:
    A. MSI_Linux_Disable_On-Access scan VSE 1.9.2
    B. MSI_Linux_Defautl_STIG Compliant VSE 1.9.2
23. Under the actions column, select Delete for each of these rules. Click OK to the confirmation message that appears for each.

Client Task Catalog Amendment:

1. Copy the entire “McAfeeMTN” folder to the desktop of the CSMS.

(Folder can be found on (KC708C06G000000000 = "Updated MOTOPATCH for McAfee XML Files)

2. From the top left hand section, select Menu > Client Task Catalog
3. On the left hand rail, under Client Task Types, click the arrow to the left of VirusScan Enterprise for Linux 1.9.2 / 2.0.3.
4. Result: Change VSEL Administrator’s Password and On Demand Scan appear.
5. Select On Demand Scan to display the associated tasks.
6. Under the Name column, identify the task titled, *MSI_Daily_Scan_RHEL_VSEL_1.9.2*.
7. For *MSI_Daily_Scan_RHEL_VSEL_1.9.2*, under the Actions column, select Delete.
8. Result: You will be displayed with a message warning you that deleting the task will affect the X number of systems. This is expected.
9. Click OK to continue.
10. Result: The Client Task Catalog page will refresh, and the task will be gone.
11. Under the Name column, identify the task titled, *MSI_Weekly_Scan_RHEL_VSEL_1.9.2*.
12. For *MSI_Weekly_Scan_RHEL_VSEL_1.9.2*, under the Actions column, select Delete.
13. Result: You will be displayed with a message warning you that deleting the task will affect the X number of systems. This is expected.
14. Click OK to continue.
15. Under the Name column, identify the task titled, *MSI_Manual_Scan_RHEL_VSEL_1.9.2*.
16. For *MSI_Manual_Scan_RHEL_VSEL_1.9.2*, under the Actions column, select Delete.
17. Result: You will be displayed with a message warning you that deleting the task will affect the X number of systems. This is expected.
18. Click OK to continue.
19. Result: The Client Task Catalog page will refresh, and the task will be gone.
20. From the bottom left hand section of the page, select Task Catalog Actions, and select Import.

Result: The Import Task window will appear.

21. Click Browse.

Result: Choose file to upload

22. Copy the entire “McAFeeMTN” folder to the desktop of the CSMS*.
23. Navigate to the CSMS desktop where you copied the McAfeeMTN folder.
24. Select “MSI_ClientTaskCatalogImport.xml”, and select Open.
25. Click OK to continue.

Result: The Client Task Catalog appears, showing Client Tasks to choose for import.

26. Uncheck the box in the upper left hand corner.

Result: No tasks should be selected.

27. Under the name column, identify the two task highlighted in gray, named MSI_Manual_Scan_RHEL_VSEL_1.9.2 and MSI_Weekly_Scan_RHEL_VSEL_1.9.2
28. Ensure that the Conflict column for the above tasks, reports false.

If the value reports True, please repeat the steps above to delete the Client Tasks (steps 6-17 of this section)

29. Select by placing a check mark next to MSI_Manual_Scan_RHEL_VSEL_1.9.2 and MSI_Weekly_Scan_RHEL_VSEL_1.9.2.

30. Click OK to continue.
    Result: The MSI_Manual_Scan_RHEL_VSEL_1.9.2 and MSI_Weekly_Scan_RHEL_VSEL_1.9.2 are imported and appear in the client task catalog page.
31. To verify the import was successful, ensure the Assignments column displays none.
32. From the top left hand section, select Menu > Client Task Assignments
33. Click the Action drop down at the bottom of the page, and select Import Assignments.

Result: The Client Task Importer page appears

34. Select Browse.

Result: A Choose File to Upload window appears

35. Navigate to the desktop of the CSMS where you copied the McAfeeMTN folder.
36. Select " MSI_TaskAssignmentImport.xml"
37. Click Open
38. Click Next to continue.
39. Uncheck the box in the upper left hand corner.

Result: No tasks should be selected.

40. Click Next to continue.
41. At the top left hand side of the page, uncheck the box for all items.

Result: No items will be checked.

42. Find all client task assignments with **VirusScan Enterprise for Linux 1.9.2 / 2.0.3** listed in the **Product** column, and check the box to mark for import. There should be 14 client tasks assignments matching this criteria.
43. Verify that there are NO items checked, that are listed as a conflict.
44. Click Save to import and process Client Task Assignments.

Result: The page refreshes and the Client Task Assignment page appears. This completes the Client Task Catalog Section

Enforce Policy and Task Assignment Update to System

1. From the top action bar, select System Tree.
2. Click on the Systems tab.
3. Ensure that My Organization is select on the left hand rail.
   (selected means highlighted in yellow)
4. On the right hand pane, with Systems tab open, use the Preset drop down, to select:
   This Group and All Subgroups.

Result: Your systems managed by ePO appear.

5. Below the Preset drop down field, find the check box in the same row with the column header labels. (should be next to column labeled, *DNS Name*)
6. Place a check in the box. This will select all systems.

Result: The selected rows will turn yellow, and a checkmark will be present in next to all systems.

7. Use the scroll bar on the right hand side to navigate to the bottom of the page.
8. From the bottom of the page, find and click the *Wake Up Agents* box.

Result: The Wake Up McAfee Agent page will appear, displaying multiple rows of settings.

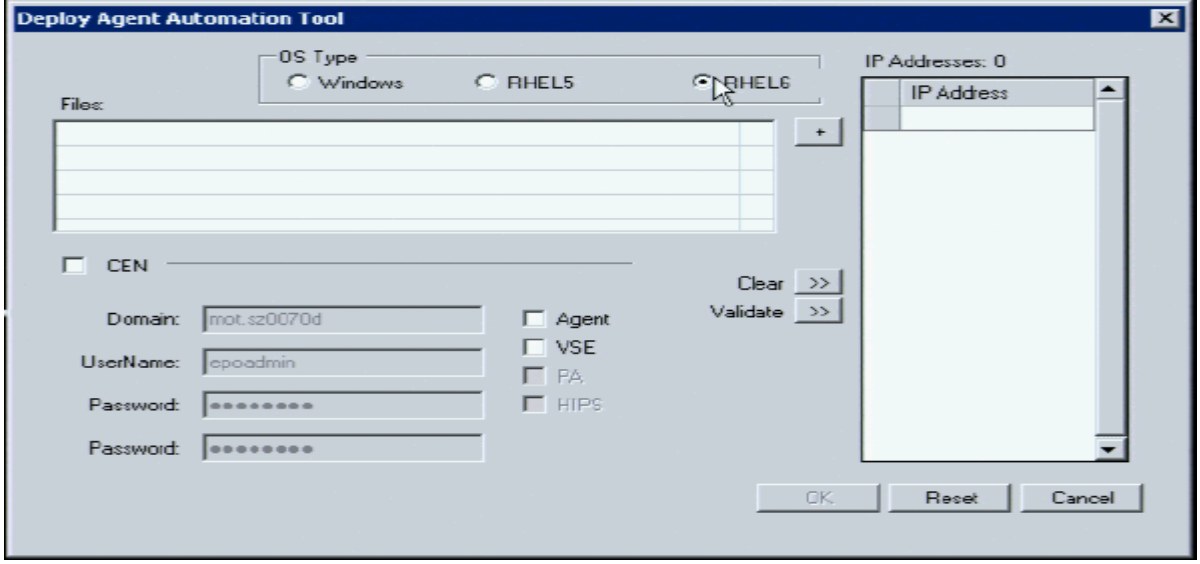
9. Find the row labeled, *Force Policy Update*.
10. Place a check mark in the box to **Force complete policy and task update.**
11. Click OK at the bottom right hand side of the page.

Result: The page will refresh and return back to the System Tree Page. In the background , the ePO server is waking the McAfee agents across the system, and applying and enforcing the VSEL Policy changes that were just amended..

12. Click on Menu> Automation> Server Task Log.
13. Under the Name column, confirm that you see an entry for Wake Up Agents, with status of *Completed 100%.*

Deploy VSEL 1.9.2 to the 7.16 ATR (applicable to 7.16 systems only)

1. Log on to the CSMS using a domain account with administrative rights.
2. Double click on "Deploy_McAfee_Agent" icon from the desktop
3. In the "User Access Control" enter a domain administrator userid and password and click "yes"
4. In the "Deploy Agent Automation Tool" window, for "OS Type" "RHEL6"



5. Select the “Agent” and “VSE” check box.
6. a. To deploy the Agent and VSE to single RHEL5, or RHEL6 container, enter a single IP address in the “IP Address” text box. Verify the settings are correct and then click “Ok” at the bottom of the window.
7. b. To deploy the Agent and VSE to the ATR, start by entering the IP address in the “IP Address” box. After the address has been entered, press the “Tab” key on the keyboard. The OK button will become available.
8. Once you have completed entering the IP addresses to deploy the Agent and VSE to the ATR, click “OK” at the bottom of the window.
9. Observe the status window for the Deploy_Agent Script. Once the installation has successfully completed, you may close out of the window.

If any failures appear, please contact your System Administrator or the Motorola SSC.

10. This may take up to 10 minutes to complete.
11. Log into the ATR device with the appropriate domain account.
12. Elevate to root user, by typing *su* – and then the appropriate password.
13. To verify success, type the following command to ensure that VSEL 1.9.2 installed:
    #/opt/NAI/LinuxShield/bin/nails --version

You should see the following version appear on the first line of text:

McAfeeVSEForLinux 1.9.2.29197-29197-noarch

14. To finalize the installation without rebooting the server, you must restart the Nails service. To do this:

From the ATR prompt as root, type the following command

/etc/init.d/nails -restart

15. You will observe the McAfee VSE monitor gateway and daemon perform a stop, and then perform a start.
16. Once this completes successfully, you will return to prompt.

(This will address the ATR RCM application connection issue

RESOLUTIONS AND REPAIR PROCEDURES:

Upgrade to the appropriate version as listed in the “PARTS REQUIRED (HARDWARE/SOFTWARE):” section below, based on the model and perform tasks described in the Workaround

To obtain software:

1. Initiate a software request case through Motorola Solution, Inc. System Support Center (SSC) at 1-800-221-7144 (1-302-444-9800)
2. Await confirmation email from UOST with instructions
3. Complete the Upgrade Operations Software Team (UOST) Software Order Form:
    a. Reference **MTNxxxx** 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.
4. Email completed Software Order Form to UOST for processing

PARTS REQUIRED (HARDWARE/SOFTWARE):

KC708C06G000000000 - Updated MOTOPATCH for McAfee XML Files

ADDITIONAL INFORMATION:

Security Update Service (SUS) customers should download “KC708C06G000000000 - Updated MOTOPATCH for McAfee XML Files” directly from the SUS website, where SUS products are normally acquired.

REFERENCE THE FOLLOWING DOCUMENTS/PROCESSES FOR INSTALLATION PROCEDURES:

None

WHEN TO APPLY RESOLUTION:

After reboot __
After (re)installation __
After upgrade __
After power cycle __
After database restoration __
After failure __
On FRU replacement __
During maintenance __
Immediately _x_
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 centre
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 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: _____

Software Description _____

Part# or Version # _____

Quantity: _____