MOTOROLA SOLUTIONS

DOCUMENT NUMBER: MTN-0027-21-NA
APC: 877
ISSUE DATE: 04-2021
EXPIRATION DATE: 30-04-2022
Bulletin Type: Informational Only

Motorola Solutions Technical Notification (MTN)

TITLE: McAfee VSE Scanners Consuming RHEL CPU and Memory - Impacts to Call Processing

TECHNOLOGY: ASTRO 25

SYMPTOMS:

Call Processing Symptoms:

1. Radios may receive bonks
2. The ZC links to the other devices (RF sites, consoles, conventional, etc.) may bounce

Other Symptoms:

1. RHEL-based applications enter malfunction state, become slow, or unresponsive

MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED:

A7.17.2 and prior RHEL devices with McAfee VSE installed. The issue affects ASTRO systems that have mismatched VSE DAT and engine files. Systems with SUS subscriptions have a higher chance of having a DAT-to-engine mismatch if DAT updates are being applied without the appropriate engine updates. NOTE: SUS provides updated engines in its service, so the reasons for missing engine updates could be due to following procedures incorrectly or technical issues with the engine download.

SEVERITY RECOMMENDATION:

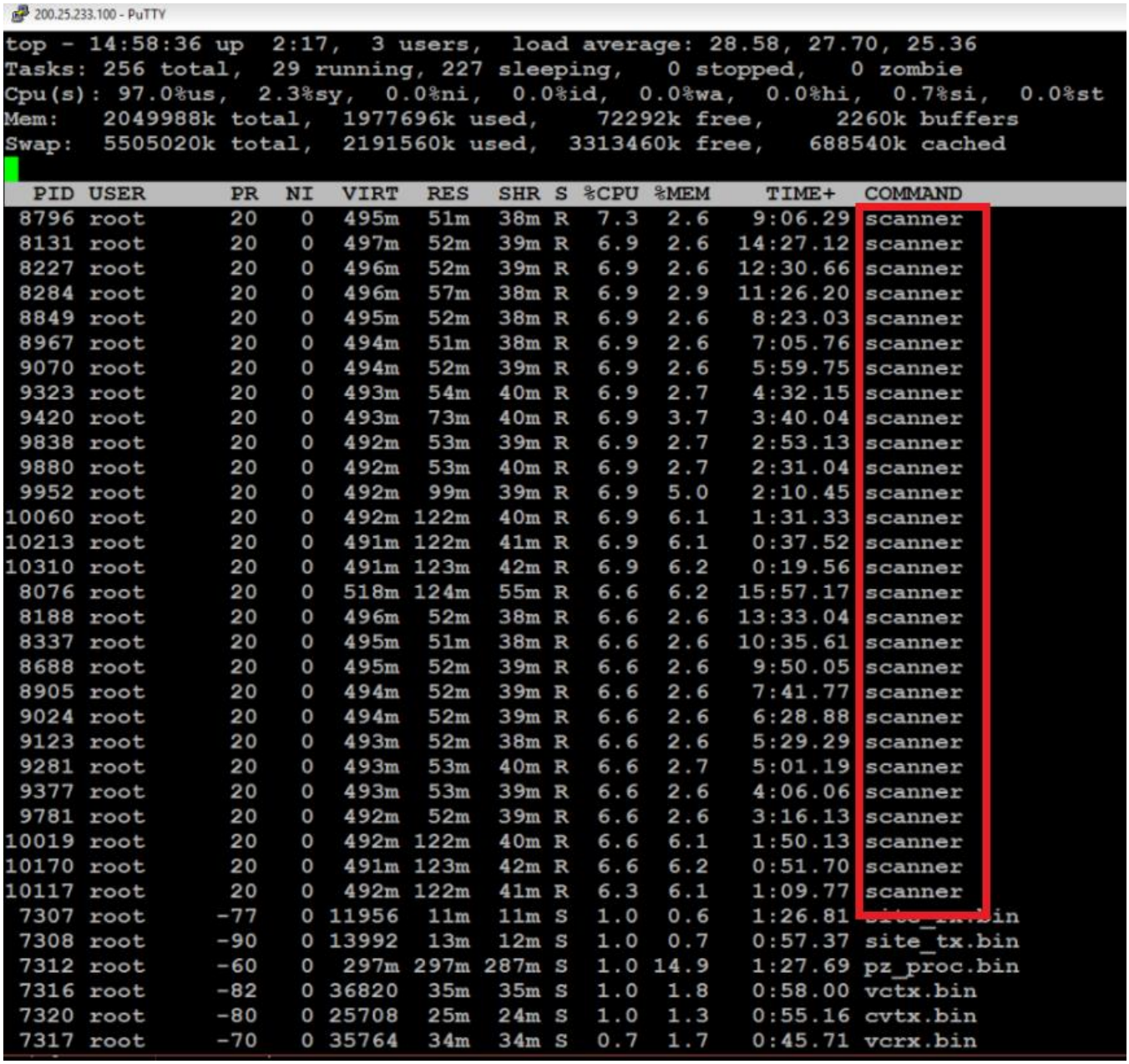
Medium / Operational - Schedule to implement

ROOT CAUSE / DEFINITIVE TEST:

Definitive Test that Issue is Actively Occurring:

McAfee VSE scanner processes do not successfully initialize or close. This allows the processes to accumulate in number and resources consumed (e.g. high CPU utilization).

1. Login to the RHEL VM with administrative privileges
2. Perform the following command: `top` and see if multiple processes named “scanner” are running. You can press ‘`P`’ to filter on the processes taking the most CPU. If everything is OK, only one “scanner” process will be running as root. If multiple “scanner” processes are running as root (see image below) then the issue in this MTN is being observed. Furthermore if a scan is running as nails user, this is a true scan that is expected to run weekly but never on ZC, PDG, or ISGW.



3. If you see multiple scanner processes running as root, you'll have to apply the **Immediate Corrective Action #1** for effected RHEL boxes to address the actively occurring issue and then subsequently check the **Corrective Actions #2 - 4** to prevent it from happening again in the future.

Test that Linux Device is Prone to the Issue:

1. **From Linux:**
    a. Login to the RHEL VM with administrative privileges
    b. Perform the following command: `/opt/NAI/LinuxShield/bin/nails --version`

```
(zc01.zone1):(root) 21:37:21 CST ZC-Astro-07.16.00.59-06
# /opt/NAI/LinuxShield/bin/nails --version
McAfeeVSEForLinux 1.9.1.29107-29107-noarch
Virus definition files 9905.0000
Virus scanning engine 5700.7163
Virus scanning engine API 5700.7163
Apache 2.4.2 (Unix)
OpenSSL 1.0.1j 15 Oct 2014
sqlite 2.8.17
```

    c. Take note of the **Virus definition files** value and the **Virus scanning engine** value and see Step 3.
2. **From CSMS/ePO:**
    a. Login to the CSMS VM with administrative privileges.
    b. Login to the McAfee ePO application using the shortcut on the desktop.

c. Click the **Menu** (top left) and click **Master Repository** (under the *Software* section)
d. Verify that both **DAT** and **Linux Engine** rows exist *and* are marked as being on the *Current* branch.
e. Take note of both **Versions** (both *DAT* and *Linux Engine*).
    i. If **Linux Engine** is missing entirely *and* the system is participating in Motorola's Weekly Vetted Antivirus Definitions SUS Subscription, the system may be prone to the issue described in this MTN. **Corrective Action #2** below must be followed.
    ii. If **Linux Engine** is missing entirely *but* the system *does not* participate in Motorola's Weekly Vetted Antivirus Definitions SUS Subscription, the system is likely not prone to the issue described in this MTN and it's not necessarily a bad thing that your Linux Engine is not displayed (you still have a Linux Engine being deployed, it's just not visible in the Master Repository)
    iii. Finally, if **Linux Engine** and **DAT** are both present, take note of their versions and see Step 3.

3. Assessing DAT vs Engine Version

a. Although not an exact science, compare the engine version to the DAT version you noted in Steps 1 or 2. For a given Engine, check to see if your DAT falls roughly within the estimated supported range. If your DAT falls far outside of the estimated range, there could be chances of resource issues noted in this MTN, so it's recommended to check **Corrective Action #2**, **#3**, and **#4**

Engine	Rough Estimate Supported DAT Range	Engine End of Life Status
5700	7719 - 8062	2/29/2016
5800	7901 - 8637	9/6/2017
5900	8509 - 9238	4/30/2019
6000	9027 - 9816	11/28/2020
6010	9399 - 9816	11/28/2020
6100	9632 +	Soon
6200	9828 +	Current

b. NOTE: The middle column is just an estimate, intended to help give a sense of the range, they should not be considered hard cutoffs. This table is a snapshot in time, for the most up to date info on McAfee VSE Engines, see https://kc.mcafee.com/corporate/index?page=content&id=KB66741

WORKAROUNDS AND CORRECTIVE ACTIONS:

Immediate Corrective Action #1 - Multiple Scanner Processes Running as Root

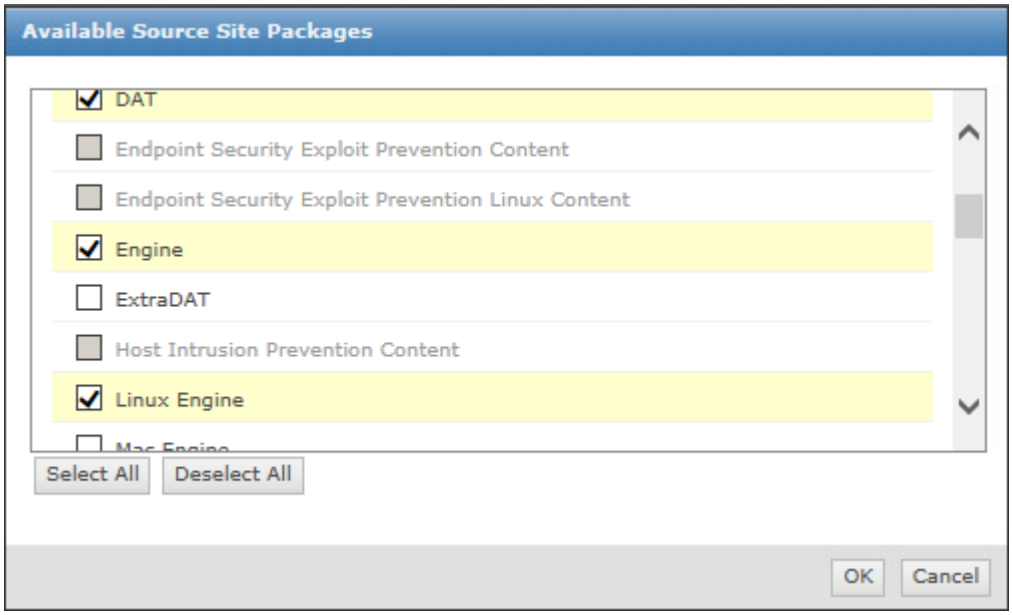
1. Check the running scanner processes with: `ps -ef | grep -i scanner`
2. Kill the scanner processes with: `killall -KILL scanner`
3. KEEP IN MIND: these scanner processes can start returning after this point and up until your Engine is updated, so you may have to return to this procedure one last time after your Engine is updated in order to kill any extra scanner processes one last time.

Corrective Action #2 - Missing Linux Engine for AV Definition SUS Service

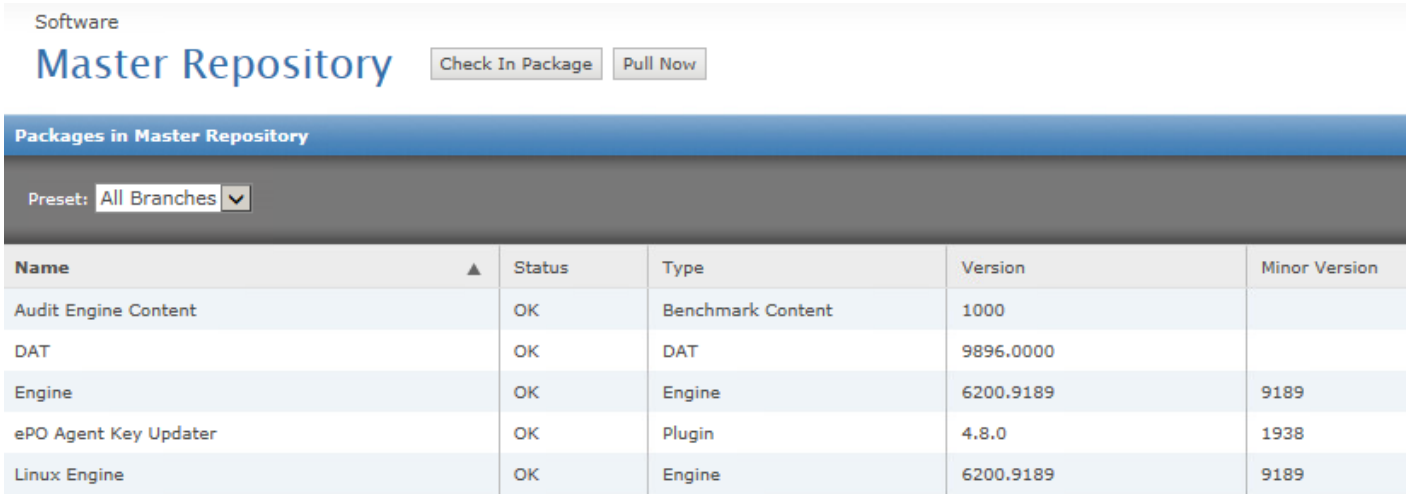
NOTE: If the system is participating in the AV Definition SUS service it's expected that the AVVDAT_<date>.zip contents have been appropriately extracted to the C:\McAfee-Updates folder on CSMS according to the McAfee Anti-Virus Manual

1. Login to the CSMS VM with administrative privileges.
2. Login to the McAfee ePO application using the shortcut on the desktop.
3. Click the **Menu** (top left) and click **Server Tasks** (under the *Automation* section)
4. Find the **Update Master Repository** task and click **Edit** (in the right-hand column)
5. Click the second tab called **2 Actions** (or click the **Next** button on the bottom right)
6. Click the **Select Packages** button and ensure that the **DAT**, **Engine**, and **Linux Engine** packages are selected with a check mark. NOTE: This step is dependent on the source site being appropriately staged (either the connection to "SSC McAfee Updater Server" is complete or the C:\McAfee-Updates is populated with the extracted AVVDAT_<date>.zip

contents). If not correctly staged, these checkboxes may be greyed out preventing you from selecting them.



7. Click **OK**
8. Click **Save** (on the bottom right)
9. Back on the *Server Tasks* page, find the **Update Master Repository** task and click **Run** (in the right-hand column)
10. You'll be brought to the *Server Task Log* page. Ensure the task completes successfully (you may have to refresh the page).
11. Once complete, click **Menu** (top left) and click **Master Repository** (under the *Software* section)
12. Ensure **Linux Engine** is now present



Name	Status	Type	Version	Minor Version
Audit Engine Content	OK	Benchmark Content	1000	
DAT	OK	DAT	9896.0000	
Engine	OK	Engine	6200.9189	9189
ePO Agent Key Updater	OK	Plugin	4.8.0	1938
Linux Engine	OK	Engine	6200.9189	9189

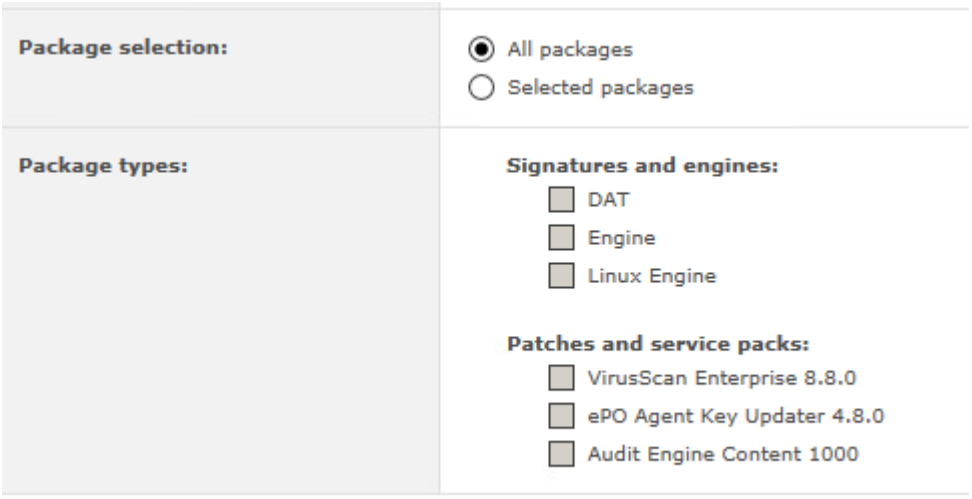
13. Continue to **Corrective Action #2**

Corrective Action #3 - Client Task

Once the appropriate software is present in the Master Repository, it then needs to be distributed out to the McAfee Agents. That's done through the Client Task.

1. In ePO, click **Menu** and click **Client Task Catalog** (under the *Policy* section)
2. In the left pane, under *McAfee Agent* click **Product Update**
3. In the right pane, find **MSI_DAT_Update** and click it.

4. Ensure that **Package Selection** is set to **All Packages**



5. If modified, click **Save**
6. This client task runs automatically every day (e.g. 4:30 AM) and causes the McAfee Agents to download the available software from the Master Repo. If you don't want to wait, you can manually trigger this task using the remainder of this procedure.
7. Login to the RHEL VM with administrative privileges
8. Perform the following command: `/opt/NAI/LinuxShield/bin/nails task --list`

```
(zc01.zone1):(root) 22:42:41 CST ZC-Astro-07.16.00.59-06
# /opt/NAI/LinuxShield/bin/nails task --list
LinuxShield configured tasks:
     1  "LinuxShield Update"  (Running)
```

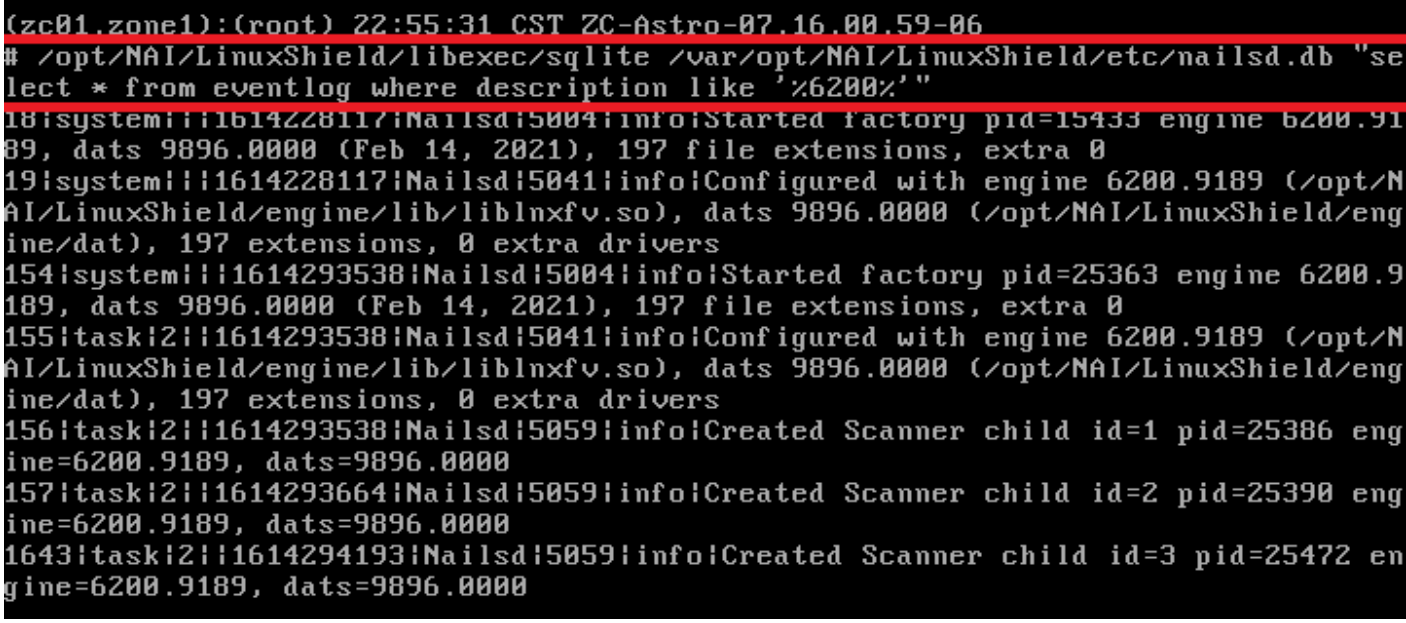
9. Take note of the number before the "LinuxShield Update" task. In this example, '1'. Most likely yours won't be "Running" at this time.
10. Perform the following command: `/opt/NAI/LinuxShield/bin/nails task -r <client task id>`
11. Continue to **Corrective Action #3**

Corrective Action #4 - Verify DAT and Engine Updates have Occurred

1. Login to the RHEL VM with administrative privileges
2. Perform the following command: `grep -i engine: /opt/McAfee/cma/scratch/etc/log` It's possible that your McAfee Agent version is different so in that case, use: `/opt/NAI/LinuxShield/libexec/sqlite /var/opt/NAI/LinuxShield/etc/nailsd.db "select * from eventlog where description like '%<engine_version>%'"`

```
(zc01.zone1):(root) 22:21:46 CST ZC-Astro-07.16.00.59-06
# grep -i engine: /opt/McAfee/cma/scratch/etc/log
2021-02-24 21:46:22 [12222]  (638997)  [UpdEvents] [I] Generating update event:E
ventId=2401:Severity=4:ProductId=LYNXSHLD1700:Locale=0000:UpdateType=Engine:Upda
teError=0:NewVersion=6100.8979:DateTime=
2021-02-24 21:46:37 [12222]  (638997)     [muemsg] [I] Update succeeded to versi
on Engine: 6100.8979 DAT: 9905.0000.
2021-02-24 22:23:02 [13052]  (720915)  [UpdEvents] [I] Generating update event:E
ventId=2401:Severity=4:ProductId=LYNXSHLD1700:Locale=0000:UpdateType=Engine:Upda
teError=0:NewVersion=6200.9189:DateTime=
2021-02-24 22:23:34 [13052]  (720915)     [muemsg] [I] Update succeeded to versi
on Engine: 6200.9189 DAT: 9896.0000.
2021-02-24 22:41:26 [15399]  (835606)  [UpdEvents] [I] Generating update event:E
ventId=2401:Severity=4:ProductId=LYNXSHLD1700:Locale=0000:UpdateType=Engine:Upda
teError=0:NewVersion=6200.9189:DateTime=
2021-02-24 22:41:57 [15399]  (835606)     [muemsg] [I] Update succeeded to versi
on Engine: 6200.9189 DAT: 9896.0000.
```

Ensure that you see "successful" events and the DAT and Linux Engine version you have in the Master Repository.



Ensure that you see processes using the latest scan engine.

3. Return once more to **Immediate Corrective Action #1** to check for and kill any malformed scanner processes that may have started in the duration leading up to the Engine update.

RESOLUTIONS AND REPAIR PROCEDURES:

None. See *WORKAROUNDS AND CORRECTIVE ACTIONS* Section.

Upgrade to the appropriate version as listed in the "PARTS REQUIRED (HARDWARE/SOFTWARE):" section below, based on the model.

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 Motorola Solutions Software Factory with instructions
3) Complete the Motorola Solutions Software Factory Software Order Form:
   a) Reference MTN-0027-21-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.
4) Email completed Software Order Form to MSSF for processing

PARTS REQUIRED (HARDWARE/SOFTWARE):

If a subscriber to Motorola's Weekly Vetted Antivirus Definitions SUS Subscription, you may need to download the latest AVVDAT_<date>.zip file from the SUS site.

ADDITIONAL INFORMATION:

None.

REFERENCE THE FOLLOWING DOCUMENTS/PROCESSES FOR INSTALLATION PROCEDURES:

SUS' McAfee Anti-Virus Manual

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 __
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

Software Order Form

Motorola Solutions Software Factory

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: _____

_____

_____

Email: _____

Attn: _____

Phone: _____

Bill To: _____

_____

_____

_____

Attn: _____

Phone: _____

Customer Billing

P.O. #: _____

CUST #: _____

TAG #: _____

Internal Billing

PROJECT #: _____

FSB #: _____

DEPT #: _____

APC #: _____

MOTOROLA SOLUTIONS

Software Order Form

Motorola Solutions Software Factory Phone Number: (800) 221-7144

° This form has been sent to you because you have requested an order from the *Motorola Solutions Software Factory* Team.

° Please fill out the order form and email back to the *Motorola Solutions Software Factory* 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 is SSA CUSTOMER please order via Motorola factory order.
2) Limited Liability is Implied to the maximum of order amount.
3) Price quotes provided by SCHSWF 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: _____