DOCUMENT NUMBER: MTN-0062A-20-NA
APC: 877
ISSUE DATE: 02-2022
EXPIRATION DATE: 28-02-2023
Bulletin Type: Informational Only

Motorola Solutions Technical Notification (MTN)

TITLE: Memory Leak in McAfee Endpoint Security (ENS) for Linux

TECHNOLOGY: ASTRO25

SYMPTOMS:
Symptoms that may be seen include

- PDG (or generically RHEL devices) runs out of memory
  - PDR loses connection to RNG
- ADS link down between ZDS and Ops
- ADS link down between ZDS and ATR
- ADS link down between ZDS and ZCs
- Unable to access/login to ZDS

MODELS / SYSTEM RELEASES / KITS / DATECODES AFFECTED:
RHEL devices with McAfee ENSLTP (Endpoint Security Linux Threat Prevention) version 10.6.2 installed

CSMS / McAfee Models Affected by this MTN
Models (Linux) with Endpoint Security (ENS) 10.6.2 and prior will get ENS replaced by a newer version:

- Linux (M-Core and L-Core)
  - PDG, ZDS, BAR, SYSLOG, ZSS, ZC, License Manager, etc.

Models (CSMS) will have its configuration updated to support the new version of ENSLTP:

- CSMS (M-Core and L-Core)
  - CSMS will have new ENSLTP packages installed in ePO
  - CSMS will have Client Tasks updated in ePO to distribute the new ENSLTP

For ZDS, reference MTN-0036-20-NA_ZDS for a complete fix (additional ZDS-specific steps).

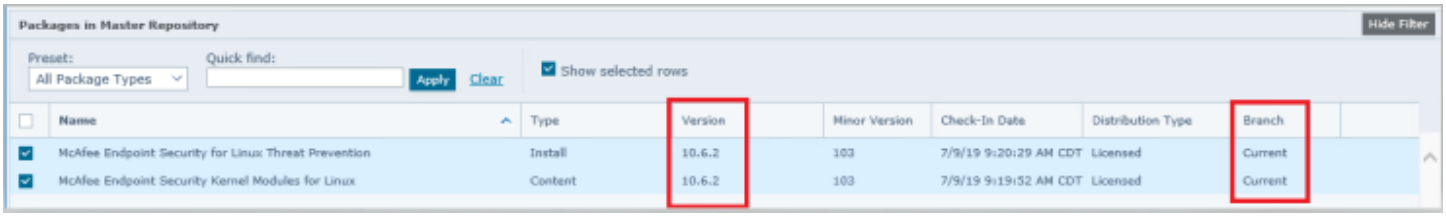
System Releases Affected:

- ASTRO® 25 System Releases A7.17.0 - A2019.2 that match the “Definitive Test for Checking ENS for Linux Version” below

Definitive Test for Checking ENS for Linux Version

Steps to check ENS for Linux packages versions:

- Log in to the McAfee ePolicy Orchestrator X.X.X Console on the CSMS
  - Double click “**Launch McAfee ePolicy Orchestrator x.x.x Console**” icon on the desktop of the CSMS
  - Enter **User name** and **Password** credentials for ePO to login.
- Click the **Menu Button** (3 horizontal lines)
- Select **Master Repository** under **Software**
- Look for the modules **McAfee Endpoint Security for Linux Threat Prevention** and **McAfee Endpoint Security Kernel Modules for Linux**
- Note down the **Version** and **Branch** for these two modules.



- If McAfee ENSLTP (Endpoint Security Linux Threat Prevention) is greater than 10.6.2, you do not need to apply this MTN.
- If McAfee ENSLTP (Endpoint Security Linux Threat Prevention) is 10.6.2 or lower, you need to apply this MTN.

SEVERITY RECOMMENDATION:
Medium / Operational - Schedule to implement

Root Cause:
A memory leak present in McAfee ENSLTP 10.6.2 (delivered via CSMS) installed on RHEL devices depletes resources over time and may eventually impact the application on that RHEL device.

To determine if your system is affected please check the Definitive Test for Checking ENS for Linux Version above.

WORKAROUNDS AND CORRECTIVE ACTIONS:.

See the “Resolutions and Repair Procedures” section below.

RESOLUTIONS AND REPAIR PROCEDURES:

1. Perform the procedure in Appendix A
2. If McAfee Agent is not 5.6.1 or greater, as returned in Appendix A, perform the procedure in Appendix B.
3. If McAfee Agent is 5.6.1 or greater, as returned in Appendix A, perform the procedure in Appendix C.

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 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-0062A-20-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):

- A7.17.3 - A2019.2 CSMS Configuration Media (Non-SA CSMS CONFIG) (KC877V0C4000000108)

ADDITIONAL INFORMATION:
Approximate time to apply this MTN: 30 minutes

If MTN-0062 was already applied and no issues are seen then this MTN is not necessary, however there are additional cleanup steps that may be useful.

REFERENCE THE FOLLOWING DOCUMENTS/PROCESSES FOR INSTALLATION PROCEDURES:
General CSMS Manuals:

- A7.17.3 Core Security Management Server Feature Guide (MN004873A01)
- A7.18 Core Security Management Server Feature Guide (MN005338A01)
- A2019.2 Core Security Management Server Feature Guide (MN005942A01)

WHEN TO APPLY RESOLUTION:
As instructed _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-topics.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

Appendix A – Definitive Test for Checking Agent for Linux Version

Steps to check ENS for Linux packages versions:

- Log in to the McAfee ePolicy Orchestrator X.X.X Console on the CSMS
  - Double click "**Launch McAfee ePolicy Orchestrator x.x.x Console**" icon on the desktop of the CSMS
  - Enter **User name** and **Password** credentials for ePO to login.
- Click the **Menu Button** (3 horizontal lines)
- Select **Master Repository** under **Software**
- Look for the module **McAfee Agent for LINUX**
- Note down the **Version** and **Branch** for this module.

- If McAfee Agent is not 5.6.1 or greater, move to Appendix B next.
- If McAfee Agent is 5.6.1 or greater, move to Appendix C next.

Appendix B – Installing Agent and ENS Extensions and deploying

Repair Procedures for Agent and ENS for Linux / CSMS

Prerequisites:

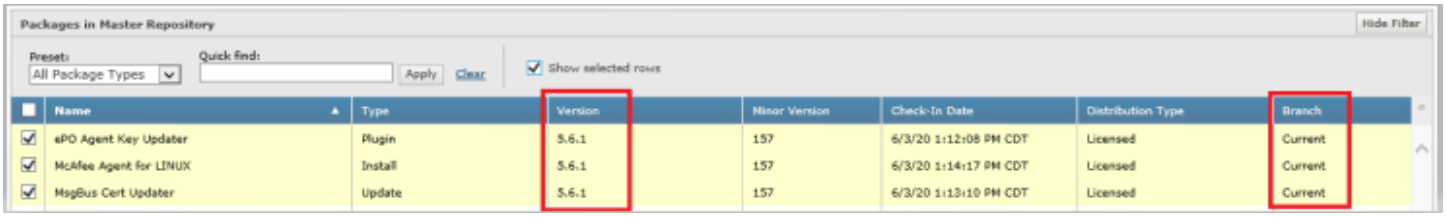
- Obtain the admin credentials for CSMS.
- Obtain the admin credentials for ePO.
- Obtain a copy of the CSMS Configuration Media (see PARTS REQUIRED (HARDWARE/SOFTWARE) section

Procedure:

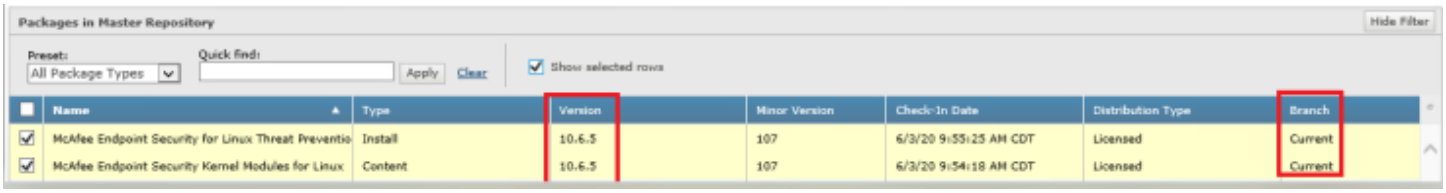
1. Import Extension Packages
   a. Mount the CSMS Configuration Media to the CSMS
   b. Log into the CSMS with administration rights
   c. Open **File Explorer**
   d. Navigate to the **DVD-ROM Drive** labeled **CSMS-Confguration_Media**
   e. Copy **CSMS_Package_Installer folder** to Desktop
   f. Double click "**Launch McAfee ePolicy Orchestrator x.x.x Console**" to open up the McAfee ePO Console.
   g. An Internet Explorer window will open to the McAfee ePolicy Orchestrator log-in window
   h. Enter **User name** and **Password** credentials for ePO to login.
   i. Once logged in click the **Menu Button** (3 horizontal lines)
   j. Under **Software**, select **Extensions**
   k. Click the **Install Extension** button
   l. Click **Browse** and navigate to the **CSMS_Package_Installer** folder on the desktop.
   m. Select **EPOAGENTMETA.zip**
   n. Select **Open**
   o. On the Install Extension window select **OK**.
   p. Select **OK** on the Extensions screen.
   q. Click the **Install Extension** button
   r. Click **Browse** and navigate to the **CSMS_Package_Installer** folder on the desktop.
   s. Select **help_ma_560.zip**
   t. Select **Open**
   u. On the Install Extension window select **OK**.
   v. Select **OK** on the Extensions screen.
   w. Click the **Install Extension** button
   x. Click Browse and navigate to the **CSMS_Package_Installer** folder on the desktop.
   y. Select **Extensions\10.6.1** folder
   z. Select **Endpoint_Security_Platform_10.6.1_1295_Extension.zip**
   aa. Select **Open**
   bb. On the Install Extension window select **OK**.
   cc. Select **OK** on the Extensions screen.
   dd. Click the **Install Extension** button

ee. Click Browse and navigate to the **CSMS_Package_Installer** folder on the desktop.
ff. Select **Extensions\10.6.1** folder
gg. Select **Threat_Prevention_10.6.1.1364_Extension.zip**
hh. Select **Open**
ii. On the Install Extension window select **OK**.
jj. Select **OK** on the Extensions screen.
kk. Click the **Install Extension** button
ll. Click Browse and navigate to the **CSMS_Package_Installer** folder on the desktop.
mm. Select **Extensions\10.6.1** folder
nn. Select **Web_Control_10.6.1.1261_Extension.zip**
oo. Select **Open**
pp. On the Install Extension window select **OK**.
qq. Select **OK** on the Extensions screen.
rr. Click the **Install Extension** button
ss. Click Browse and navigate to the **CSMS_Package_Installer** folder on the desktop.
tt. Select **ENDPL_LIC-10.6.5-Build_101(Extension).zip**
uu. Select **Open**
vv. On the Install Extension window select **OK**.
ww. Select **OK** on the Extensions screen.

2. Run the CSMS Package Installer Script
   a. Open Powershell:
      i. From **Start**, type in powershell
      ii. Right click **Windows Powershell**, run as administrator
      iii. In the User Account Control dialog box, click **Yes**
   b. At the prompt, enter cd 'C:\Users\<Administrator>\Desktop\CSMS_Package_Installer'
   c. Enter .\CSMS_package_installer.ps1
   d. You will be asked for the ePO Web Interface Credentials, enter the ePO credentials obtained in the prerequisites and select **OK**.
   e. Once you see "**CSMS_package_installer.ps1 completed successfully**" the script has finished.
   f. Exit Powershell
   g. Verify the new packages were installed in the CSMS
      i. Log in to the McAfee ePolicy Orchestrator X.X.X Console on the CSMS
         1. Double click "**Launch McAfee ePolicy Orchestrator x.x.x Console**" icon on the desktop of the CSMS
         2. Enter **User name** and **Password** credentials for ePO to login.
      ii. Click the **Menu Button** (3 horizontal lines)
      iii. Select **Master Repository**
      iv. Look for the modules **ePO Agent Key Updater, McAfee Agent for Linux** and **MsgBus Cert Updater**
      v. Look at the columns **Version** and **Branch** for these modules.
      vi. The Version should now be **5.6.1** on the **Current** branch.



      vii. In the Master Repository, look for the modules **McAfee Endpoint Security for Linux Threat Prevention** and **McAfee Endpoint Security Kernel Modules for Linux**
      viii. Look at the columns **Version** and **Branch** for these two modules.



      ix. The **Version** should now be **10.6.5** on the **Current** branch, as shown above.
      x. Remove any older versions of **McAfee Endpoint Security for Linux Threat Prevention** and **McAfee Endpoint Security Kernel Modules for Linux** that are older than **10.6.5**.
         1. If there are any **McAfee Endpoint Security for Linux Threat Prevention** and **McAfee Endpoint Security Kernel Modules for Linux** that are older than 10.6.5, click the check box next to them.
         2. Click **Actions** drop down at bottom of the screen
         3. Select **Delete Package**

4. Select **OK** in the confirmation screen.

3. Remove **McAfee Agent for Linux** from **Previous** branch
    a. Click the **Menu Button** (3 horizontal lines)
    b. Select **Master Repository**
    c. Look for the module **McAfee Agent for Linux**
    d. Look at the columns **Version** and **Branch**
    e. If there is an entry of **McAfee Agent for Linux** on a **Branch** other than **Current**, do the following:
        i. Click the box next to the entry for **McAfee Agent for Linux** that is not on **Current**
        ii. Click **Actions** drop down at bottom of the screen
        iii. Select **Delete Package**
        iv. Select **OK** in the confirmation screen.
4. New Client Tasks, **MSI: Deploy McAfee Agent 5.6.1.157 to Linux** and **ENSLTP 10.6.5 Update** have been added to the system. **MSI: Deploy McAfee Agent 5.6.1.157 to Linux** has been run on all Linux hosts in the system.
5. Wait two hours for deployment to Linux devices to finish.
6. Run Query to check progress of installation of Agent on Linux hosts.
    a. In **ePO**, navigate to **Menu > Reporting > Queries & Reports**
    b. Under **Groups** on the left select **Shared Groups > MSI**
    c. Find the query "**MSI: List Managed system with Linux**"
    d. In the **Actions** column click **Run**
    e. This Query will list all Linux systems along with the **Product Version** of **Agent** and **Endpoint Security Platform**, you can refresh this page to refresh the values in the **Product Version** columns.
    f. As the **Product Version (Agent)** is updated to **5.6.1.157** you can deploy **ENS for Linux** via the following method.
        i. Select the Linux devices you want to push ENS to by selecting the checkbox next to the name, only do this for the devices that have **Product Version (Agent)** of **5.6.1.157**.
        ii. Select **Actions** at the bottom of the screen and navigate to **Agent > Run Client Task Now**
        iii. Under **Product** select **McAfee Agent**
        iv. Under **Task Type** select **Product Deployment**
        v. Under **Task Name** select **ENSLTP 10.6.5 Update**
        vi. Click the **Options** tab
        vii. In **Randomization** enter 120 next to minutes.
        viii. Click **Run Task Now**.
        ix. The **Running Client Task Status** window will appear which will give the Status of all the systems chosen and their progress.
    g. Repeat step e to verify all Linux hosts have had Agent and Endpoint Security Platform Versions updated. Please note that due to the Randomization it could take up to 2 hours for all Linux hosts to be updated.

Appendix C – Procedure for Updating ENS for Linux Version

Repair Procedures for ENS for Linux / CSMS

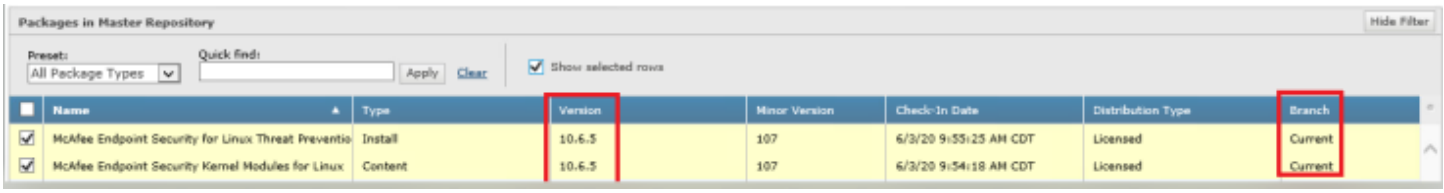
Prerequisites:

- Obtain the admin credentials for CSMS.
- Obtain the admin credentials for ePO.
- Obtain a copy of the CSMS Configuration Media (see PARTS REQUIRED (HARDWARE/SOFTWARE) section

Procedure:

1. Import ENS Extension Package
    a. Mount the CSMS Configuration Media to the CSMS
    b. Log into the CSMS with administration rights
    c. Open **File Explorer**
    d. Navigate to the **DVD-ROM Drive** labeled **CSMS-Confguration_Media**
    e. Copy **CSMS_Package_Installer folder** to Desktop
    f. Double click "**Launch McAfee ePolicy Orchestrator x.x.x Console**" to open up the McAfee ePO Console.
    g. An Internet Explorer window will open to the McAfee ePolicy Orchestrator log-in window
    h. Enter **User name** and **Password** credentials for ePO to login.
    i. Once logged in click the **Menu Button** (3 horizontal lines)
    j. Under **Software**, select **Extensions**.
    k. Click the **Install Extension** button
    l. Click Browse and navigate to the **CSMS_Package_Installer** folder on the desktop.
    m. Select **Extensions\10.6.1** folder
    n. Select **Endpoint_Security_Platform_10.6.1_1295_Extension.zip**
    o. Select **Open**
    p. On the Install Extension window select **OK**.
    q. Select **OK** on the Extensions screen.
    r. Click the **Install Extension** button
    s. Click Browse and navigate to the **CSMS_Package_Installer** folder on the desktop.
    t. Select **Extensions\10.6.1** folder
    u. Select **Threat_Prevention_10.6.1.1364_Extension.zip**
    v. Select **Open**
    w. On the Install Extension window select **OK**.
    x. Select **OK** on the Extensions screen.
    y. Click the **Install Extension** button
    z. Click Browse and navigate to the **CSMS_Package_Installer** folder on the desktop.
    aa. Select **Extensions\10.6.1** folder
    bb. Select **Web_Control_10.6.1.1261_Extension.zip**
    cc. Select **Open**
    dd. On the Install Extension window select **OK**.
    ee. Select **OK** on the Extensions screen.
    ff. Click the **Install Extension** button
    gg. Click Browse and navigate to the **CSMS_Package_Installer** folder on the desktop.
    hh. Select **ENDPL_LIC-10.6.5-Build_101(Extension).zip**
    ii. Select **Open**
    jj. On the Install Extension window select **OK**.
    kk. Select **OK** on the Extensions screen.
2. Run the CSMS Package Installer Script
    a. Open Powershell:
        i. From **Start**, type in powershell
        ii. Right click **Windows Powershell**, run as administrator
        iii. In the User Account Control dialog box, click **Yes**
    b. At the prompt, enter cd 'C:\Users\<Administrator>\Desktop\CSMS_Package_Installer'
    c. Enter .\CSMS_package_installer.ps1
    d. You will be asked for the ePO Web Interface Credentials, enter the ePO credentials obtained in the prerequisites and select **OK**.
    e. Once you see "**CSMS_package_installer.ps1 completed successfully**" the script has finished.
    f. Exit Powershell
    g. Verify the new packages were installed in the CSMS
        i. Log in to the McAfee ePolicy Orchestrator X.X.X Console on the CSMS
            1. Double click "**Launch McAfee ePolicy Orchestrator x.x.x Console**" icon on the desktop of the CSMS
            2. Enter **User name** and **Password** credentials for ePO to login.
        ii. Click the **Menu Button** (3 horizontal lines)
        iii. Look for the modules **McAfee Endpoint Security for Linux Threat Prevention** and **McAfee Endpoint Security Kernel Modules for Linux**

iv. Look at the columns **Version** and **Branch** for these two modules.
v. The Version should now be **10.6.5** on the **Current** branch.
vi. Remove any older versions of **McAfee Endpoint Security for Linux Threat Prevention** and **McAfee Endpoint Security Kernel Modules for Linux** that are older than **10.6.5**.
    1. If there are any **McAfee Endpoint Security for Linux Threat Prevention** and **McAfee Endpoint Security Kernel Modules for Linux** that are older than 10.6.5, click the check box next to them.
    2. Click **Actions** drop down at bottom of the screen
    3. Select **Delete Package**
    4. Select **OK** in the confirmation screen.



3. A Client Task has been scheduled to run on all Linux Hosts. This could take up to 2 hours before all the Linux hosts have ENS upgraded successfully
4. Wait 2 hours for installations to complete.
5. Run Query to check progress of installation of ENS on Linux hosts.
    a. In **ePO**, navigate to **Menu > Reporting > Queries & Reports**
    b. Under **Groups** on the left select **Shared Groups > MSI**
    c. Find the query "**MSI: List Managed system with Linux**"
    d. In the **Actions** column click **Run**
    e. This Query will list all Linux systems along with the **Product Version** of **Agent** and **Endpoint Security Platform**, you can refresh this page to refresh the values in the **Product Version** columns. Verify that **Product Version (Endpoint Security Platform)** is updated to **10.6.5**.

This MTN includes the following software updates or configuration changes:
Software updates:

- McAfee® ePO Server will receive new packages for the following:
    - McAfee Agent for LINUX -- version 5.6.1.157
    - McAfee Endpoint Security for Linux Threat Prevention – version 10.6.5.107
    - McAfee Endpoint Security Kernel Modules for Linux – version 10.6.5.107

Configuration changes:

- McAfee ePO Server will receive an update to the following Client Tasks:
    - McAfee Agent > Product Deployment > MSI_deploy_ENS_to_RHEL
    - McAfee Agent > Product Deployment > MSI_ENS_deploy _to_RHEL_var
    - McAfee Agent > Product Deployment > MSI_REMOVE_ENS_from_RHEL
- McAfee ePO Server will receive a new Client Tasks:
    - McAfee Agent > Product Deployment > MSI: Deploy McAfee Agent 5.6.1.157 to Linux
    - McAfee Agent > Product Deployment > ENSLTP 10.6.5 Update