Installing Software Maintenance Update for log4j2 Vulnerability

Installing Software Maintenance Update on Cisco DCNM Windows and Linux Deployment

This section provides instructions to install Software Maintenance Update (SMU) on Cisco Windows and Linux deployments Release 11.5(1) to address **CVE-2021-45046** and **CVE-2021-44228** issue. Note that **CVE-2021-45105** has a lower severity and not used in DCNM with default configuration, and therefore it is not addressed here.

Note Only a **root** or **admin** user can install the SMU on the Cisco DCNM setup.

This section contains the following topics:

Installing the SMU on Cisco DCNM Windows Appliance

To install the SMU on Cisco DCNM Windows appliance, perform the following:

Before you begin

- Take a backup of the Cisco DCNM application. Copy the backup file to a safe location outside the DCNM server.
- If Cisco DCNM appliance is installed in VMware environment, ensure that you take VM snapshots for all nodes. For instructions, refer to *VMware Snapshot Support* section in your Cisco DCNM Release Notes.
- Ensure that you plan for a maintenance window to install SMU.
- Ensure that Cisco DCNM 11.5(1) is up and running.

Note Only a **root** user can install the SMU on the Cisco DCNM Release 11.5(1) appliance

Procedure

Step 1 Download the SMU file.

a) Go to the following site: https://software.cisco.com/download/.

A list of the latest release software for Cisco DCNM available for download is displayed.

b) In the Latest Releases list, choose Release 11.5(1).

c) Locate **DCNM 11.5(1) Maintenance Update for Windows and Linux Servers to address CVE-2021-45046 and CVE-2021-44228** and click Download icon.

Save the `dcnm-win-linux-patch.11.5.1.zip` file to your directory that is easy to find when you start to apply the maintenance update (patch).

Step 2 Upload the file to the **`C:\Users\<UserName>\Desktop\`** folder in the DCNM setup.

Step 3 Log on to Cisco DCNM using SSH as a **Administrator** user.

Step 4 Unzip the **`dcnm-win-linux-patch.11.5.1.zip`** file in **`c:\Users\<UserName>\Desktop\`** directory.

Step 5 Open **Command prompt** and run as **Administrator**.

Step 6 Change directory to **`/patch`** using **c:\Users\<UserName>\Desktop\patch** command.

Step 7 Apply the patch.

```
c:\Users\<UserName>\Desktop\patch> patch.bat
Enter DCNM root directory [C:\Program Files\Cisco Systems\dcm]:
c:\Users\<UserName>\Desktop\patch

"Backing up dcm.ear ..."
        1 file(s) copied.
        1 file(s) copied.

"Stopping DCNM service..."
The Cisco DCNM SAN Server service was stopped successfully.

Waiting for  0 seconds, press CTRL+C to quit ...

"Applying patch...."
Initializing, please wait...
Patching DCNM server, please wait...

"Stopping Elasticsearch...."
The Elasticsearch 6.8.3 (elasticsearch-service-x64-683) service is stopping..
The Elasticsearch 6.8.3 (elasticsearch-service-x64-683) service was stopped successfully.

Waiting for  0 seconds, press CTRL+C to quit ...
        1 file(s) copied.
        1 file(s) copied.
        1 file(s) copied.

"Starting Elasticsearch...."
The Elasticsearch 6.8.3 (elasticsearch-service-x64-683) service is starting..
```

```
The Elasticsearch 6.8.3 (elasticsearch-service-x64-683) service was started successfully.

Waiting for  0 seconds, press CTRL+C to quit ...

"Starting DCNM server..."
The Cisco DCNM SAN Server service is starting.
The Cisco DCNM SAN Server service was started successfully.
```

Installing the SMU on Cisco DCNM Linux Appliance

To install the SMU on Cisco DCNM Linux appliance, perform the following:

Before you begin

- Take a backup of the Cisco DCNM application. Copy the backup file to a safe location outside the DCNM server.
- If Cisco DCNM appliance is installed in VMware environment, ensure that you take VM snapshots for all nodes. For instructions, refer to *VMware Snapshot Support* section in your Cisco DCNM Release Notes.
- Ensure that you plan for a maintenance window to install SMU.
- Ensure that Cisco DCNM 11.5(1) is up and running.

Note Only a **root** user can install the SMU on the Cisco DCNM Release 11.5(1) appliance

Procedure

Step 1 Download the SMU file.

a) Go to the following site: https://software.cisco.com/download/.

A list of the latest release software for Cisco DCNM available for download is displayed.

b) In the Latest Releases list, choose Release 11.5(1).

c) Locate **DCNM 11.5(1) Maintenance Update for Windows and Linux Servers to address CVE-2021-45046 and CVE-2021-44228** and click Download icon.

Save the `dcnm-win-linux-patch.11.5.1.zip` file to your directory that is easy to find when you start to apply the maintenance update (patch).

Step 2 Upload the file to the **`/root/`** folder in the DCNM setup.

Step 3 Log on to Cisco DCNM using SSH as a **root** user.

Step 4 Unzip the **`dcnm-win-linux-patch.11.5.1.zip`** file in **`/root/`** directory.

Step 5 Change directory to **`/patch`**.

```
[root@dcnm]# cd patch
```

Step 6 Apply the patch.

```
[root@dcnm]# ./patch.sh
Please enter DCNM install directory.  Press Enter to select default.
[Default:/usr/local/cisco/dcm]:
DCNM Home Dir: /usr/local/cisco/dcm
Backing up dcm.ear and SanAnalytics.war...
Stopping DCNM service...
Stopping FMServer (via systemctl):   [  OK  ]
Applying patch....
Patching ear file, please wait...
Patching war file, please wait...
Stopping Elasticsearch...
Stopping elasticsearch (via systemctl):    [  OK  ]
Starting Elasticsearch...
Starting elasticsearch (via systemctl):    [  OK  ]
Starting DCNM server...
Starting FMServer (via systemctl):     [  OK  ]
```

Installing Software Maintenance Update on Cisco DCNM OVA/ISO Deployment

Cisco DCNM provides a Software Maintenance Update (SMU) to address the **CVE-2021-45046 and CVE-2021-44228** issue in Release 11.5(x). This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

This section contains the following topics:

Installing SMU on Cisco DCNM 11.5(x) Standalone Deployment

This section provides instructions to install Software Maintenance Update (SMU) on Cisco DCNM OVA/ISO appliance to address **CVE-2021-45046 and CVE-2021-44228** issue. Note that CVE-2021-45105 has a lower severity and not used in DCNM with default configuration, and therefore it is not addressed here.

To apply the Software Maintenance Update (SMU) on Cisco DCNM OVA/ISO in Standalone deployment mode, perform the following steps:

Before you begin

- Take a backup of the application data using the **appmgr backup** command on the DCNM appliance.

  ```
  dcnm# appmgr backup
  ```

  Copy the backup file to a safe location outside the DCNM server.

- If Cisco DCNM appliance is installed in VMware environment, ensure that you take VM snapshots for all nodes. For instructions, refer to *VMware Snapshot Support* section in your Cisco DCNM Release Notes.

- Ensure that you plan for a maintenance window to install SMU.

- Ensure that Cisco DCNM 11.5(x) is up and running.

  This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

Note Only a **root** user can install the SMU on the Cisco DCNM Release 11.5(x) appliance

Procedure

Step 1 Download the SMU file.

a) Go to the following site: https://software.cisco.com/download/.

A list of the latest release software for Cisco DCNM available for download is displayed.

b) In the Latest Releases list, choose Release 11.5(x).

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

c) Locate **DCNM 11.5.x Maintenance Update for VMWare, KVM, Bare-metal, and Appliance servers to address log4j2 CVE-2021-45046 and CVE-2021-44228** file and click **Download** icon.

d) Save the **dcnm-va-patch.11.5.x-p1.iso.zip** file to your directory that is easy to find when you start to apply the SMU.

Step 2 Unzip the **dcnm-va-patch.11.5.x-p1.iso.zip** file and upload the file to the `/root/` folder in the DCNM node.

Step 3 Log on to the Cisco DCNM appliance using SSH as a **sysadmin** user.

Run the **su** command to enable **root** user.

```
dcnm# su
Enter the root password:
[root@dcnm]#
```

Step 4 Run the following command to create a screen session.

```
[root@dcnm]# screen
```

This creates a session which allows you to execute the commands. The commands continue to run even when the window is not visible or if you get disconnected.

Step 5 Create a folder named **iso** using the **mkdir /mnt/iso** command.

```
[root@dcnm1]# mkdir -p /mnt/iso
```

Step 6 Mount the DCNM 11.5(x) SMU file in the `/mnt/iso` folder.

```
[root@dcnm]# mount -o loop dcnm-va-patch.11.5.x-p1.iso /mnt/iso
```

Step 7 Navigate to **/scripts/** directory.

```
[root@dcnm]# cd /mnt/iso/packaged-files/scripts/
```

Step 8 Run the **./inline-upgrade.sh** script.

```
[root@dcnm]# ./inline-upgrade.sh
```

The progress is displayed on the screen. When the installation of SMU is complete, a successful message appears.

Note After the SMU is installed successfully, the DCNM process restarts. This results in a momentary loss of access to the DCNM Web UI.

Step 9 Ensure the DCNM application is functional, by using the **appmgr status all** command.

```
[root@dcnm]# appmgr status all
```

Step 10 Terminate the **screen** session, by using the **exit** command.

```
[root@dcnm]# exit
```

Step 11 Unmount the **dcnm-va-patch.11.5.x-p1.iso** file from the DCNM setup.

Note You must terminate the **screen** session before unmounting the SMU file.

```
[root@dcnm]# umount /mnt/iso
```

Sample Output of Commands to address Log4j vulnerability

The following is a sample output while installing the SMU on Cisco DCNM Release 11.5(x).

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

Sample Output to Install SMU in DCNM Standalone Deployment

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

```
[root@dcnm]# ./inline-upgrade.sh

================================================================
============ Inline Upgrade to DCNM 11.5(x)-p1 ==============
================================================================

Upgrading from version: 11.5(x)
Upgrading from install option: LAN Fabric
System type: Standalone
Compute only: No

Do you want to continue and perform the inline upgrade to 11.5(x)-p1? [y/n]: y
==== Fri Dec 17 11:26:51 PST 2021 - Task checkAfwStatus started ====
==== Fri Dec 17 11:26:51 PST 2021 - Task checkAfwStatus finished ====
==== Fri Dec 17 11:26:51 PST 2021 - Task updateAfwApps started ====
==== Fri Dec 17 11:26:51 PST 2021 - Updating AFW applications ====
Pausing Services that need to be patched
Deleted Containers:
992d06574c57882cf1a86bf7c19414055c6f501073a262b9e97cee0a75718a55
324f8ecfc34223f9d71abb86a807af54a720b40121aa8f38f6aa2dccbc233071
f7fe8656838af352d0d128163b1e9e4dcca9e5b73ea3a0956e4199e867f69a34
ab0f0dd90b98dacca8e01c944c6b07390bad8cd8247cf8cdf7629503bd01d252
52d0d5ad7edf990424b43c57d95ba836191fa913e556e6c1b75a65f171de6be6
4daf92fd8ba5445a81913df573343c0d6617b436330d103b8abf631a477c9b91
786768ab289596fbfb3904b1115a14717057bc83a06e555aa1abb76abb4c3a9e
1f5f52c42e532b4be9cff0eb22844824d969c6838436b98251236efdf4f85f57
b780eff0776d9dfa752ef28446dcaffcffffac6ac20a2b41738ac23e6d060ed3
756097c7bd5028ee5eafc74c7fb90eae20104b1584f2611ea1b3089340d0011c

Total reclaimed space: 1.418MB
pauseAfwApp: calling PUT with  {pause}
```

```
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:26:52 GMT
Content-Length : 99
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Paused for elasticsearch_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Content-Length : 96
Content-Type : text/plain; charset=utf-8
Date : Fri, 17 Dec 2021 19:27:12 GMT
{
  "ResponseType": 0,
  "Response": "Application is Paused for watchtower_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:27:32 GMT
Content-Length : 91
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Paused for eplui_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {pause}
pauseAfwApp:  value of Wait:  false

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:27:52 GMT
Content-Length : 100
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Paused for elasticservice_Cisco_afw. Check for status"
}
Now Removing Images from Runtime
Untagged: 127.0.0.1:5001/dcnmelastic:6.8.3_11.5.2
Untagged:
127.0.0.1:5001/dcnmelastic@sha256:a872d49e3b5a0fc58ec9c1e8d8908c62604258cbfb1a02ac418227ed7f928128
Untagged: 127.0.0.1:5000/dcnmelastic:6.8.3_11.5.2
Untagged:
127.0.0.1:5000/dcnmelastic@sha256:a872d49e3b5a0fc58ec9c1e8d8908c62604258cbfb1a02ac418227ed7f928128
Untagged: dcnmelastic:6.8.3_11.5.2
Deleted: sha256:0173109c0612f48ed4165de7e5fa96f2243fe48756405bd0a0b4f12279785db1
Deleted: sha256:8d0b16f607caee532685643cf21550079881b67db9edf7d54a50ba4dec673c45
Deleted: sha256:63f9d6a3667c56f4a64d986b13b0059353fb983495b34f840b6a38c63e39938c
Deleted: sha256:af6e5eed783b56a675c53698ad4d374a77222218ebf706ad9891785b4ec2a537
Deleted: sha256:37dab1fa0ee831d1979104edd0ea820a1b3de3fe818aa75200021f868b221998
Deleted: sha256:cf1569581d9385a63ebd156e15dc795ab82de8d0a27fc5a3205dac339b591ee5
Deleted: sha256:3d293d026d9a7552a3630a75500d860083763a558191e1f28ebb6344c985b09d
Deleted: sha256:b285cfcb6bcb0850c0121d404c51ef0a333380cf332b3b776e75b45a94c2e8a7
Deleted: sha256:6e43279655973e51749e6c13dbf63733802071ff665927375f9f98827857b548
Deleted: sha256:544fc6ed244eef6449d95305179600648f339c0adbcbcbf93cc4f9e402122c53
Deleted: sha256:6810a2c88653fe864294296c70a5a657caa0f638689ff58f13493acc532f5c77
Untagged: 127.0.0.1:5001/elasticservice:1.3
Untagged:
```

```
127.0.0.1:5001/elasticservice@sha256:bf0293e69d144bbf2dbd4192f59884fb596629bb6b1b09522a75bd599b2461b2
Untagged: 127.0.0.1:5000/elasticservice:1.3
Untagged:
127.0.0.1:5000/elasticservice@sha256:bf0293e69d144bbf2dbd4192f59884fb596629bb6b1b09522a75bd599b2461b2
Untagged: elasticservice:1.3
Deleted: sha256:c6cd18e3bcc36ab60a3d741e8fa6ec166ec53de742cd959fbef572b2d6e75fdb
Deleted: sha256:be5892dd6be6e671d8dbf07949d2559cdd43ccc537a0cb4f18ee4b74f634238c
Deleted: sha256:e0f9a768f8fc9a173f00b6babcb017789713195b566f97470d9501bbbbba8e74
Deleted: sha256:213b03f962fe9b6df0da77ccabe174c74ccb790d084a25f7221076f45958ced9
Deleted: sha256:1ef5822648e60b2be83c8641db64375be04ecb6f5acd66a142919e14f8af3b4d
Untagged: 127.0.0.1:5001/watchtower:2.1
Untagged:
127.0.0.1:5001/watchtower@sha256:793aee652b615cd3161c8dd9c60eb89b6afd684fc89c6518f84ff71563bee99e
Untagged: 127.0.0.1:5000/watchtower:2.1
Untagged:
127.0.0.1:5000/watchtower@sha256:793aee652b615cd3161c8dd9c60eb89b6afd684fc89c6518f84ff71563bee99e
Untagged: watchtower:2.1
Deleted: sha256:b44bcfbcd001b7c85a2028e813ef6919e316d6af37732a092151639d1c3d2b45
Deleted: sha256:3d30de4d2f50296af6affe5baa20e58a91b84abab65f89cb379ac78308c47b1e
Deleted: sha256:a066f951d571bcead85b9a6530b14a7b82cca834a174c28de1bc037bb80a2edd
Deleted: sha256:cf95f9ed8314cec412869a95a1a50b7b7d04f29bbc5b8a3d149a424ca6c83e49
Untagged: 127.0.0.1:5001/eplui:2.2
Untagged:
127.0.0.1:5001/eplui@sha256:af90fd9362f9244ed03bdd13318f6123817a7be64e089c42f5094fd570ebb03d
Untagged: 127.0.0.1:5000/eplui:2.2
Untagged:
127.0.0.1:5000/eplui@sha256:af90fd9362f9244ed03bdd13318f6123817a7be64e089c42f5094fd570ebb03d
Untagged: eplui:2.2
Deleted: sha256:5cca4a674f345d289c814ae0a3f24ec9aac76937046beb4273b51cc29c4b6408
Deleted: sha256:d6886b2e02aaf7ebf7cfd0423bedffbd27905d12f81d0908d4ab02b2e9973cc1
Deleted: sha256:301f9eb3ba05164dbd29cab2c93dad24e5e1fea3cf2abd2f1585c25df6a75c34
Deleted: sha256:0af470c810372aa3ecee7f4f5b6cdbab0dc857ef371d658668bb43fb2e50f2ef
Checking and starting a writable registry
Error response from daemon: no such image: AfwAppRegistry: invalid reference format:
repository name must be lowercase
f11dc4cb9677d2cb7e0fe215050f69fdbb60ed583762f3867290c8ae4a712b2a
Achieved Pause state for all services, Now Patching services
Loading Images into the writable registry
Loaded image: eplui:2.2
Loaded image: dcnmelastic:6.8.3_11.5.2
Loaded image: elasticservice:1.3
Loaded image: watchtower:2.1
The push refers to a repository [127.0.0.1:5000/dcnmelastic]
97da84f99ba3: Preparing
a0bb674f2b12: Preparing
1d07ed4e39fa: Preparing
8d8a48fd5741: Preparing
b14eb3458281: Preparing
f13999d3b63e: Preparing
d1c75bcbeb10: Preparing
f51f8d284b3b: Preparing
617b86abcd6d: Preparing
d3071a656898: Preparing
0bcab5b3cf37: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
d1c75bcbeb10: Waiting
d3071a656898: Waiting
f51f8d284b3b: Waiting
5d50c3ca45af: Waiting
617b86abcd6d: Waiting
fbb373121c59: Preparing
7b9f72883f99: Preparing
9785ac5771f5: Waiting
```

```
fbb373121c59: Waiting
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
7b9f72883f99: Waiting
5fb2dee77c93: Waiting
bc2717dd2942: Waiting
0bcab5b3cf37: Waiting
1d07ed4e39fa: Pushed
97da84f99ba3: Pushed
a0bb674f2b12: Pushed
8d8a48fd5741: Pushed
b14eb3458281: Pushed
d1c75bcbeb10: Pushed
f13999d3b63e: Pushed
f51f8d284b3b: Pushed
617b86abcd6d: Pushed
d3071a656898: Layer already exists
0bcab5b3cf37: Layer already exists
5d50c3ca45af: Layer already exists
fbb373121c59: Layer already exists
9785ac5771f5: Layer already exists
7b9f72883f99: Layer already exists
5fb2dee77c93: Layer already exists
bc2717dd2942: Layer already exists
6.8.3_11.5.2: digest: sha256:0e407eefbc956a3e4c5b1705ab3add29c883e63da1b84d8e89f2345fe2fc557f
 size: 3882
The push refers to a repository [127.0.0.1:5000/elasticservice]
e9e60715acea: Preparing
83082b3681a8: Preparing
ec805d3c2de0: Preparing
fa8a90cb6518: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
fbb373121c59: Waiting
7b9f72883f99: Waiting
5fb2dee77c93: Waiting
bc2717dd2942: Waiting
9785ac5771f5: Waiting
5d50c3ca45af: Layer already exists
9785ac5771f5: Layer already exists
fbb373121c59: Layer already exists
fa8a90cb6518: Pushed
5fb2dee77c93: Layer already exists
bc2717dd2942: Layer already exists
e9e60715acea: Pushed
83082b3681a8: Pushed
7b9f72883f99: Layer already exists
ec805d3c2de0: Pushed
1.3: digest: sha256:ece5bb0b46547a166907f38f4958e40fd5202bf015728ea89dda2af342d28727 size:
 2422
The push refers to a repository [127.0.0.1:5000/watchtower]
7bb58c00bab0: Preparing
69c967d71211: Preparing
ea7268754985: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
```

```
7b9f72883f99: Waiting
5fb2dee77c93: Waiting
bc2717dd2942: Waiting
fbb373121c59: Waiting
5d50c3ca45af: Layer already exists
9785ac5771f5: Layer already exists
7b9f72883f99: Layer already exists
fbb373121c59: Layer already exists
5fb2dee77c93: Layer already exists
bc2717dd2942: Layer already exists
7bb58c00bab0: Pushed
ea7268754985: Pushed
69c967d71211: Pushed
2.1: digest: sha256:2aeded0fa00d3c92c4e78a5339eb116e27b0ac5fbed36c241fd26676a6642d91 size:
 2214
The push refers to a repository [127.0.0.1:5000/eplui]
4d33a08042c4: Preparing
a6480cd96594: Preparing
53cebfe822f4: Preparing
5d50c3ca45af: Preparing
9785ac5771f5: Preparing
fbb373121c59: Preparing
7b9f72883f99: Preparing
5fb2dee77c93: Preparing
bc2717dd2942: Preparing
7b9f72883f99: Waiting
fbb373121c59: Waiting
5fb2dee77c93: Waiting
9785ac5771f5: Layer already exists
5d50c3ca45af: Layer already exists
fbb373121c59: Layer already exists
4d33a08042c4: Pushed
53cebfe822f4: Pushed
7b9f72883f99: Layer already exists
bc2717dd2942: Layer already exists
5fb2dee77c93: Layer already exists
a6480cd96594: Pushed
2.2: digest: sha256:6a6b2266bb21bbcb88cd2fc3f01c7127d2793b663026ffa88d0665eb82f8d354 size:
 2214
AfwAppRegistry
Loaded images, now unpausing services
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:30:22 GMT
Content-Length : 100
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for elasticsearch_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:30:43 GMT
Content-Length : 97
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for watchtower_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
```

```
Date : Fri, 17 Dec 2021 19:31:04 GMT
Content-Length : 92
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for eplui_Cisco_afw. Check for status"
}
pauseAfwApp: calling PUT with  {unpause}

HTTP/1.1 200 OK
Date : Fri, 17 Dec 2021 19:31:25 GMT
Content-Length : 101
Content-Type : text/plain; charset=utf-8
{
  "ResponseType": 0,
  "Response": "Application is Running for elasticservice_Cisco_afw. Check for status"
}
Nothing to Patch in NI Base image is not installed here
==== Fri Dec 17 11:30:45 PST 2021 - Task updateAfwApps finished ====
==== Fri Dec 17 11:30:45 PST 2021 - Task disableAppsOnStandby started ====

Stopping HA apps on Standby node
Stopping AFW Applications...
Stopping AFW Server Processes
Stopping AFW Agent Processes
Stopped Application Framework...
Stopping High-Availability services: Done.

==== Fri Dec 17 11:31:45 PST 2021 - Task disableAppsOnStandby finished ====

==== Fri Dec 17 11:31:45 PST 2021 - Task stopDcnmServer started ====
==== Fri Dec 17 11:31:45 PST 2021 - Trying to upgrade your DCNM, so stopping the dcnm to
proceed... ====
Stopping FMServer (via systemctl):  [  OK  ]
==== Fri Dec 17 11:32:20 PST 2021 - Task stopDcnmServer finished ====
==== Fri Dec 17 11:32:20 PST 2021 - Task updatePackagedFiles started ====
==== Fri Dec 17 11:32:20 PST 2021 - Updating packaged-files ====
==== Fri Dec 17 11:32:20 PST 2021 - Task updatePackagedFiles finished ====
==== Fri Dec 17 11:32:20 PST 2021 - Task updateFmServer started ====
==== Fri Dec 17 11:32:20 PST 2021 - Updating FMServer ====
==== Fri Dec 17 11:32:20 PST 2021 - Backing up dcm.ear ====
==== Fri Dec 17 11:32:21 PST 2021 - Applying patch... ====
Patching ear file, please wait...
Patching war file, please wait...
==== Fri Dec 17 11:32:30 PST 2021 - Task updateFmServer finished ====
==== Fri Dec 17 11:32:30 PST 2021 - Task updatePatchList started ====
==== Fri Dec 17 11:32:30 PST 2021 - Task updatePatchList finished ====
==== Fri Dec 17 11:32:30 PST 2021 - Task startDcnmServer started ====
Started AFW Server Processes
Started AFW Agent Processes
Started applications managed by heartbeat..
Check the status using 'appmgr status all'
Starting High-Availability services: INFO:  Resource is stopped
Done.

==== Fri Dec 17 11:33:23 PST 2021 - Task startDcnmServer finished ====
==== Fri Dec 17 11:33:23 PST 2021 - Task completeUpgrade started ====

********************************************************************************
Inline upgrade of this Standalone DCNM node is complete.

==== Sat Dec 17 11:33:23 PST 2021 - Task completeUpgrade finished ====
********************************************************************************
```

Scanning for Log4j2 Vulnerabilities

Download a scanner (such as logpresso) from https://github.com/logpresso/CVE-2021-44228-Scanner.

Warning Use this utility only to scan for vulnerabilities. DO NOT use it to fix anything in the system.

Caution After installing the SMU, ensure that the DCNM Web UI is up and running. Also, ensure that all the processes are up and running, by using the **appmgr status all** command. Ensure that the **Applications > Compute** shows all nodes in **Joined** state.

Before running the scan again, clear the old docker images that are no longer used, by using the following command:

If **docker ps -a** shows many containers in Exited state, then first run the following:

```
docker container prune
WARNING! This will remove all stopped containers.
Are you sure you want to continue? [y/N] y
Deleted Containers:
33d2a44706663870d062b7ee8b4aba18ea94ea6fdc285b6ba1d133334f226d73
9fba3140120f7fbc41993a97d0bc6bec254ffed638da1445e3a91fb04614cba6
67d4cd575d1febdec54fe161d716334908eb18d1a9a5d053a8f21ed1e3089d8c
4b8f2463cf899341fd5a028078a3d6b98790807db1ba6f6ece13a5a0a7783749
5b066b6eb334986d0cb0442249218d8582936439f8c8b3a3c81426ab81beaac3
14b965917498dcaaaa3e586d0d65e702d884c3cef7e425e60215a192cbff9945
359ab2ca568d10c42e406fec6a6f7499637936080b0ca109e307c51ca9431532
a18a752de7208d3802989f9209893140cac404cf33dcdf5cb362ebbddbde4e04
519e0e7654ecff8601f868c2a55fd1507a9ce52d137c33c79067fe3d7f834048
03e0c0ccaa35e2b4d07c6afae90c758f3db5ea639528afcc550a26e9c1ef1b43
Total reclaimed space: 155.4MB
```

If there are no containers in Exited state, then you can directly run the **docker image prune** to clean up the old images, as follows:

```
docker image prune -a
WARNING! This will remove all images without at least one container associated to them.
Are you sure you want to continue? [y/N] y
Deleted Images:
untagged: 127.0.0.1:5001/eplui:2.1
untagged:
127.0.0.1:5001/eplui@sha256:6b788e837561f5b56378d9872885abd078105b6e18f17f8b28ff7d58106288ed
deleted: sha256:9a9bb56bcf9e5807e25743522e7cc3b7946ca39b875418b5f85894b383443276
deleted: sha256:d09c3547766a3130d2e48d85d5c33304fd912abbcc0fd8f6d877ca4a5a7513d8
deleted: sha256:19acc971e6674459c817bd011ed8e5969bc4f47f3f733fe9ffb617227d5081e0
deleted: sha256:5f5a7996ee7ba7d79772caa9a24f95cceb8463bab030c7ed8f534b14eda099db
untagged: 127.0.0.1:5001/elasticservice:1.1
untagged:
127.0.0.1:5001/elasticservice@sha256:b7b7a082aa225301e92c55ab93647a7f4e5b49e28152733075995a6b237aa798
deleted: sha256:f9078f534739f1367d9a67187f14f4c32cc9fc904c8fd6579564c848b06f9185
deleted: sha256:f0e44e2f9afc9e180056d5bc6fceed743c2d2e4936a71ae8feb2c5e317ccea25
deleted: sha256:0cab6e9119a4779b58e3f8a2ab48ec892db599ca53a784a63ed2d03aa422a87e
deleted: sha256:60546313de31095f5363f479ea12b74ff02375f96cb5ab5ba23e85027f3be2c4
deleted: sha256:c9d22e3ec2ce60122c9da1d8e8bafb18dd9b61db39c3e8e8ad70be6ec907c48c
untagged: dcnmelastic:6.8.3_11.4.1
deleted: sha256:9e6493318e1189b662683cb288532e9b3177464684e9c17f06ebcd1a6bd3c317
deleted: sha256:f1b3c86a97ad0767ffcc89c31b73d34643a2bb838e317c82f00167bb8cfb270e
deleted: sha256:19c89e64341aff41ec5508ebb2b73107fee9581d71d78b0787279817dd14facc
```

```
deleted: sha256:907f6e93fa619661d70a65dc3fd12d0257e3d7afb0ced3961620fa419c5dd792
deleted: sha256:044e562105291191158e417ae9d33dd16022a881562114a970d1fadb116e8e5a
deleted: sha256:48c418ce6e32de81f4171ae073e79b04b3c227afe5f4013e6a0bd5932eee3853
deleted: sha256:7b6c7e6083bffb94f1b9acd4f83acec0f4cdc0685efda47fb6a9735fb0c3ec65
deleted: sha256:59908c99dea86854472cb0d7b64236e4a903f815d652845f56ec30204a12f550
deleted: sha256:11124a752156a4ec945d79172f11be3f025c96f1989886dff9b0b3608303dc3e
untagged: kibana:2.0
deleted: sha256:ea95ed7a67f68301e64e46653af6864cb6e18e496e725432505595936b560f26
deleted: sha256:b153b99c46885f4cd2b05173fb1b5481bda9f10c39130e5cbb38b7cd18884508
deleted: sha256:02033d4e0a299ba71df33ceaff68959d74d4a62fc0be69b689a01e6322f8e64c
deleted: sha256:9ed6d76808f43ff63909ba38cdda9430109b4848c4cb5b7e8db63e9a9f5e9f7e
deleted: sha256:c4ca19d8d6603e6020c28b9eefba5fe056bab61099a7c15a1b0793281601ea54
deleted: sha256:eac1498f3113436c89751c285e6d52c13edfa05810abce2dc042c9750f4b64b6
deleted: sha256:5f265142267b87373fafa5ccff18c1d7f2c7ce8b25ad870263dba4a9ff3a8540
deleted: sha256:f98eb78bb8712f2786ef0580037d916d4ff0d3bf398900f093c94301cad4d705
deleted: sha256:6262d3d4d32bb0a107cfac0c58c563426fdc657116c903e36334a452a4818d68
deleted: sha256:045f4e8b3ed31fb7d27aa34e59cfdd2e8aa5b24d9cde5b84de18635a5b7f3765
deleted: sha256:af643141c457d060c8c88f4b3901d8404bab5b93abdcba1c5050666de50765e2
untagged: watchtower:2.1
deleted: sha256:0a54bd9e96a8483fdb76042b7906909aa1f3fd4deb513a5a7194a8aaf86af7dc
deleted: sha256:f8f11cb198e25e36212a5650d5b8fbcc9f4a515afe91e6d4e678d71c60d6040d
deleted: sha256:224ec704095b7d5d185a405f0e468bc015d6cb9c50cd3ab4ca9de092763ddc5a
deleted: sha256:45268517a253b8f483eedfa7f9f2641361d3f40d5e6f235f179ee3f583ebfc38
untagged: compliance:4.0.0
deleted: sha256:d6750c132fb5e9059f86d0d6b1f54bebd0f00d0b84ab9688813526bd63c6ced8
deleted: sha256:4d10e42b5db7aafabef673b889c6916e79c9f1cf6a5411304b02e158dfac0cbc
deleted: sha256:7ffadb4dd9f304c2d5314f66461d351622fe72e6c2a043942e0cd7fcc8aa2b66
deleted: sha256:516e697bbb7ff9ec971280964b9383fa22cc72ced415362720903ad5281c0852
deleted: sha256:0ef534a6e063d02b7bc5f1ff0a0053478502a8bc76f88cd2dddb58b8225c80a4
deleted: sha256:4a7f56d08ea1e6fcda2d9fd2b37c85eee0e963c9d8c6275997a4028171a15c07
deleted: sha256:544c874de2ace981da4bd06ee33cd8a00d03059b598cc4a02fc4ab9b57610133
deleted: sha256:5f0a9421371e6f218eaf9788eccfc987d40cc7c66291536465f271cf0abdcd04
deleted: sha256:c1968f6e62beccbad147b8f8d0a239b4d308133ee0bc77cd4ee9cfc941f29e50
deleted: sha256:aa9e87a76c7b54bb7dba91db45a84a23542bf647751fe1211764f1395f97ec6f
Total reclaimed space: 794.1MB
```

After that, the log4j scanner tool can be run. A sample post patch run output is depicted below:

CLI snap of a sample result - CVE-2021-44228 Vulnerability Scanner 2.3.6 (2021-12-20)

```
[root@dcnm]# ./log4j2-scan /
Logpresso CVE-2021-44228 Vulnerability Scanner 2.3.6 (2021-12-20)
Scanning directory: /, ./log4j2-scan, / (without devtmpfs, tmpfs, shm)
Running scan (10s): scanned 4653 directories, 41925 files, last visit:
/usr/local/cisco/dcm/fm/download
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/sandeployments/dcm.ear
(lib/log4j-core-2.16.0.jar), log4j 2.16.0
Running scan (26s): scanned 6980 directories, 62226 files, last visit:
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/sandeployments
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/tmp/vfs/deployment/deployment8b48896c390adc/log4j-core-2.16.0.jar-f0e635d46279bf/log4j-core-2.16.0.jar,
 log4j 2.16.0
Running scan (36s): scanned 9856 directories, 90359 files, last visit:
/usr/local/cisco/dcm/wildfly-14.0.1.Final/modules/system/layers/base/org/infinispan/main
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/root/packaged-files/pmn/pmn-telemetry.jar, log4j 2.16.0
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in /root/patch-11.4.1-p2.backup/dcm.ear
 (lib/log4j-core-2.8.2.jar), log4j 2.8.2
Running scan (52s): scanned 24714 directories, 141807 files, last visit:
/root/patch-11.4.1-p2.backup
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/tmp/.inline-upgrade.16121/fmserver-patch/log4j-core-2.16.0.jar, log4j 2.16.0
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/tmp/.inline-upgrade.16121/fmserver-patch/dcm.ear (lib/log4j-core-2.16.0.jar), log4j 2.16.0
```

```
Running scan (62s): scanned 30813 directories, 183000 files, last visit:
/usr/share/elasticsearch/modules/lang-groovy
Running scan (72s): scanned 34709 directories, 216946 files, last visit:
/usr/local/cisco/dcm/smis/client/lib
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/sandeployments/dcm.ear
(lib/log4j-core-2.16.0.jar), log4j 2.16.0
Running scan (88s): scanned 36975 directories, 231284 files, last visit:
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/sandeployments
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/usr/local/cisco/dcm/wildfly-14.0.1.Final/standalone/tmp/vfs/deployment/deployment8b48c896c390adc/log4j-core-2.16.0.jar-f0e635d46279bf/log4j-core-2.16.0.jar,
 log4j 2.16.0
Running scan (98s): scanned 39835 directories, 259398 files, last visit:
/usr/local/cisco/dcm/wildfly-14.0.1.Final/modules/system/layers/base/org/bouncycastle/main
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/root/packaged-files/pmn/pmn-telemetry.jar, log4j 2.16.0
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in /root/patch-11.4.1-p2.backup/dcm.ear
 (lib/log4j-core-2.8.2.jar), log4j 2.8.2
Running scan (114s): scanned 54709 directories, 310865 files, last visit:
/root/patch-11.4.1-p2.backup
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/tmp/.inline-upgrade.16121/fmserver-patch/log4j-core-2.16.0.jar, log4j 2.16.0
[*] Found CVE-2021-45105 (log4j 2.x) vulnerability in
/tmp/.inline-upgrade.16121/fmserver-patch/dcm.ear (lib/log4j-core-2.16.0.jar), log4j 2.16.0
Scanned 59990 directories and 338115 files
Found 12 vulnerable files
Found 0 potentially vulnerable files
Found 0 mitigated files
Completed in 124.16 seconds
```

Note Installing SMU on Cisco DCNM addresses CVE-2021-44228 and CVE-2021-45046. As CVE-2021-45105 is lower severity, and refers to an issue with a configuration which is not used in Cisco DCNM with the default shipping configuration. Therefore, CVE-2021-45105 is not addressed in this SMU installation.

The backup contains original unaltered files which are still vulnerable. They are not used, but are retained as a reference. If you choose to delete, no functionality will be impacted. There are few files which are inside of container filesystem layers. These files record the changes to the container filesystems and are not a concern until they do not appear in the “merged” container files. These files are not available to processes at run-time. There are no vulnerable files in the merged resultant container filesystems.

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

Refer to Upgrading DCNM Release 11.5(x) from Previous Versions, on page 15 for instructions to install SMU on other DCNM releases. You can upgrade to DCNM Releases through multiple hops from Release 11.0 or later. The log4j2 scanner flags few stale docker/overlay related file system issues. Ensure that you validate the SMU installation. For more information, see Validating of SMU Installation, on page 15.

Note After DCNM HA failover, the log4j2 scan may show some vulnerabilities. This is due to the old docker image package bundle in the Standby server, which is not available for use at run-time for any process. If the CVE reports are still seen, execute the **docker image prune -a** command. This results in clearing the stale entries on the Standby node. After clearing stale entries, there will be no issues during further DCNM HA failovers. If the scan report still shows some CVE errors, we recommend that you contact Cisco TAC.

Validating of SMU Installation

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

To validate that the patch has been successfully applied on Cisco DCNM appliances, check the contents of the file located at **/root/packaged-files/properties/dcnm-version.txt**. If the patch is successfully applied, an extra line is included in the dcnm-version.txt as shown below:

PATCH_LIST=X

where,

X is the number of patches installed on your Cisco DCNM appliance.

Note After the SMU is installed, the **Health Monitor** application (previously known as **Watchtower**) will not display any old or new data.

Upgrading DCNM Release 11.5(x) from Previous Versions

When upgrading from an older DCNM 11.x version to 11.5(x) or higher, post upgrade and patch application, the log4j scanner may show more vulnerabilities related to findings in the **/var/lib/docker/overlay** file system. A sample output of a system upgraded from DCNM 11.2(1) to 11.5(1) is shown below after installing the SMU. The sample output shows multiple vulnerabilities all in the docker/overlay file system. The two vulnerabilities seen for **docker/overlay2** filesystem for elasticsearch doesn't cause any issues.

This SMU installation is supported with Release 11.5(1), 11.5(2), and 11.5(3) for your deployment.

```
./log4j2-scan /
Logpresso CVE-2021-44228 Vulnerability Scanner 2.2.0 (2021-12-18)
Scanning directory: / (without devtmpfs, tmpfs, shm)
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in
/var/lib/docker/overlay/2a7db7cebfce3ac7ca67206122b55e813ea19801593c433b5fd730c69d0a1b69/root/
usr/share/elasticsearch/lib/log4j-core-2.9.1.jar, log4j 2.9.1
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in /var/lib/docker/overlay/2811b1325950ad4c
438cdd1b2631adb0a1adfa0b49e474279f3499cfd2e49ad3/root/usr/share/elasticsearch/lib/log4j-core-2.9.1.jar,
 log4j 2.9.1
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in
/var/lib/docker/overlay/8b6416f75366e50688
1755714e39a6f23e581bb5886386eaab935f5d8ed923ad/root/usr/share/elasticsearch/lib/log4j-core-2.9.1.jar,
 log4j 2.9.1
.
..
...
Running scan (95s): scanned 223603 directories, 1965175 files, last visit:
/tmp/.inline-upgrade.11270/fmserver-patch
Running scan (107s): scanned 236660 directories, 2034298 files, last visit:
/usr/local/cisco/dcm/
wildfly-14.0.1.Final/standalone/sandeployments
[*] Found CVE-2021-44228 (log4j 2.x) vulnerability in /root/patch-11.5.1-p1.backup/dcm.ear
 (lib/
log4j-core-2.8.2.jar), log4j 2.8.2
Running scan (117s): scanned 243726 directories, 2095783 files, last visit:
/root/patch-11.5.1-p1.backup
Scanned 243914 directories and 2096444 files
Found 29 vulnerable files
Found 0 potentially vulnerable files
```

```
Found 0 mitigated files
Completed in 117.36 seconds
```

From DCNM release 11.3(1), the Application Framework uses the overlay2 file system for docker. You can verify by using the following command:

```
docker info | grep overlay2
Storage Driver: overlay2              /* above command must display this output*/
```

If the output of the above command indicates docker is using **overlay2**, the directory **/var/lib/docker/overlay** is not used, and therefore, the errors reported by scanner are remnants, and not used by any running service on the DCNM. To cleanup these remnants, please do the following on the node where errors are reported.

Remove the remnants on the node where additional vulnerabilities are reported by using the following command:

```
rm -rf /var/lib/docker/overlay
```

Caution Ensure that you execute the above command correctly. If overlay2 is deleted accidentally, the DCNM services will not be operational.

Run the log4j scanner. The displayed output shows that all the vulnerabilities related to **/var/lib/docker/overlay** are removed.