Product Support Notice

PSN #	PSN027079u

Original publication date: 21-Mar-19. This is Issue #13, published date: 21-Mar-24.

Severity/risk level	High	Urgency	Immediately

Name of problem	PSN027079u- Avaya Solutions Platform 130 R4.0 Dell® R640 Customized Image of VMware ESXi 6.5 - *EOMS Oct 15, 2022*

Products affected

Avaya Solutions Platform 130 Dell® R640

NOTE: Avaya Converged Platform (ACP) was rebranded to Avaya Solutions Platform in December of 2019

Problem description

UPDATE MARCH 21, 2024: Clarification -- Installation/Upgrade instructions in this PSN are for updates within ASP 4.x (ESXi 6.5) and maintained for historical purposes. All upgrades from ASP 4.x to ASP 5.x require that the ASP 4.x server be on the latest available Avaya customized release *VMware-Dell-Customized-ESXi6.5u3-19092475.*
Beginning with ASP 5.1.0.3, customers that are on R4.0 (ESXi 6.5 – must be on latest release Build #19092475) or R5.0 (ESXi 7.0U2) must conduct a step-up upgrade to R5.1, R5.1.0.1 or R5.1.0.2 first before upgrading to R5.1.0.3. Supported upgrade paths are documented in the ASP Release Notes.
All upgrades from ASP 4.x to ASP 5.x require review of the relevant ASP 5.1.x documents, including PCNs, Release Notes, specific Upgrade documents. Ensure BIOS/Firmware is on the latest Avaya certified version. Always check support.avaya.com for the latest documents.

UPDATE OCTOBER 7, 2022: With VMware ESXi 6.5 End of General Support on October 15, 2022 and Avaya's previously announced *End of Sale (EOS) and End of Manufacturer Support (EOMS)* with EOMS effective October 15, 2022, Avaya Solutions Platform 130 R4.0 customers should update to the latest Avaya Solutions Platform R5.1 which utilizes ESXi 7.0. This will ensure continuation of Avaya support for security updates on ESXi. Servers currently on ASP R4.0 (ESXi 6.5) must be on the latest available Avaya customized release, *VMware-Dell-Customized-ESXi6.5u3-19092475.* **before updating to ASP 5.x Reference *PCN2146Su* *Avaya Solutions Platform 130 5.1* for details on ASP 5.1. Applications running on ASP 130 must be reviewed for compatibility with ESXi 7.0 and may require an update to the latest supported application release. For example, Aura 7.1.x (EOMS December 2020) applications on ASP 130 R4 will need to update to an Aura release that is compatible with ESXi 7.0. As a best practice, software currency is always recommended and customers should update to the latest available application version. Reference individual product application documentation for details.**

Following information maintained for historical purposes.

This PSN will be used to track updates of any new Avaya approved/certified Dell® R640 customized image of VMware ESXi 6.5 for installation on the ASP 130 Dell® R640. The ASP 130 R640 comes pre-loaded with a customized image of VMware ESXi 6.5.

This is ONLY applicable to ASP 130 and should not be used for other ASP server models (ASP 110, ASP 120).
Avaya Solutions Platform 130 Dell® R640 servers are supplied under OEM relationship and managed differently than commercially available servers from the vendor. Support, warranty and repair are through Avaya's processes, not through the OEM vendor's support process.

Only Avaya provided updates can be used. Updating directly from the Dell or VMware's web sites will result in an unsupported configuration.

This PSN allows customers to update their existing servers to the latest certified R4.0 (ESXi 6.5) build.
Note that the OEM server vendor (in this case Dell) provides Avaya with their latest certified package of the ESXi 6.5 software. This ensures that any updates will be compatible with the underlying hardware, drivers, etc.
Beginning with the June 2022 update, the ESXi 6.5 19092475 build (ESXi650-202202001.zip) from VMware was used to begin the file customization. VIBs were imported from Dell EMC A08 add-on, but if VIBs/drivers were newer in the ESXi image, the newer versions were used.
Once Avaya has an update from the vendor, the new image is fully vetted with the Avaya solutions to assess any potential performance or capacity impacts. This image is then made available on plds.avaya.com and is customer installable.

Date	Customized Version of VMware ESXi 6.5 Dell Release Notes Link/VMware Release Notes Link starting June 2022	ISO Image File Name (for recovery only) PLDS ID	Zip File Name (for update from previous version) PLDS ID
July 2018	**ESXi 6.5 U2** A00, Build#8294253	VMware-VMvisor-Installer-6.5.0.update02-8294253.x86_64-DellEMC_Customized-A00.iso **PLDS ID:** ACP0000005	N/A
March 2019	**ESXi 6.5 U2** A07, Build#10719125 ESXi_65U2-ReleaseNotes-DellEMC-A07.txt	VMware-VMvisor-Installer-6.5.0.update02-10719125.x86_64-DellEMC_Customized-A07.iso **PLDS ID:** ACP0000004	VMware-VMvisor-Installer-6.5.0.update02-10719125.x86_64-DellEMC_Customized-A07.zip **PLDS ID:** ACP0000003
December 2019	**ESXi 6.5 U2** A12, Build#13635690 ESXi_65U2-ReleaseNotes-DellEMC-A12.txt	VMware-VMvisor-Installer-6.5.0.update02-13635690.x86_64-DellEMC_Customized-A12.iso **PLDS ID:** ACP0000006	VMware-VMvisor-Installer-6.5.0.update02-13635690.x86_64-DellEMC_Customized-A12.zip **PLDS ID:** ACP0000007
October 2020	**ESXi 6.5 U3** **A05 Build#15256549** ESXi_65U3-ReleaseNotes-DellEMC-A05.txt	VMware-VMvisor-Installer-6.5.0.update03-15256549.x86_64-DellEMC_Customized-A05.iso **PLDS ID:** ACP0000009	VMware-VMvisor-Installer-6.5.0.update03-15256549.x86_64-DellEMC_Customized-A05.zip **PLDS ID:** ACP0000010
June 2021	**ESXi 6.5 U3** A06 build#17167537 ESXi_65U3-ReleaseNotes-DellEMC-A06.txt	VMware-VMvisor-Installer-6.5.0.update03-17167537.x86_64-DellEMC_Customized-A06.iso **PLDS ID:** ACP0000012	VMware-VMvisor-Installer-6.5.0.update03-17167537.x86_64-DellEMC_Customized-A06.zip **PLDS ID:** ACP0000013
October 2021	**ESXi 6.5 U3** A07 Build#17477841 ESXi_65U3-ReleaseNotes-DellEMC-A07.txt	VMware-VMvisor-Installer-6.5.0.update03-17477841.x86_64-DellEMC_Customized-A07.iso **PLDS ID:** ACP0000015	VMware-VMvisor-Installer-6.5.0.update03-17477841.x86_64-DellEMC_Customized-A07.zip **PLDS ID:** ACP0000016
June 2022	**ESXi 6.5 U3** Build#19092475 ESXi 6.5, Patch Release ESXi650-2022-02001 Release Notes **Process change:** Previous updates utilized the Dell EMC Custom image. With the June 2022 image, the ESXi 6.5 19092475 build (ESXi650-202202001.zip) from VMware was used to begin the file customization. VIBs were imported from Dell EMC A08 add-on, but if VIBs/drivers were newer in the ESXi image, the newer versions were used.	VMware-Dell-Customized-ESXi6.5u3-19092475.iso **PLDS ID:** ACP0000017 **Note**: Different file name format beginning June 2022.	VMware-Dell-Customized-ESXi6.5u3-19092475.zip **PLDS ID:** ACP0000018 **Note**: Requires different update command from previous versions. See the Resolution section of this PSN for details. **Note**: Different file name format beginning June 2022.

The zip file is used to update from the previous installed image.
The iso image is for recovery purposes only in the event a server needs to be reinstalled in the field.

For a server reinstall, the ISO images below can be utilized and the “Performing server recovery or software remastering” section of the *Installing the Avaya Converged Platform 130 Series* Release 4.0 document should be referenced.

Resolution

Acquiring the latest Dell Customized Image for updates

Login to plds.avaya.com and download the corresponding version of the Dell Customized Image of VMware ESXi 6.5 identified in the table above. Use the zip file for updates, the iso image for a server reinstall.

Installing the latest Dell Customized Image for updates

NOTE: Different update command needed beginning with June 2022 zip file. Previous update command should still be used for all pre-June 2022 updates.

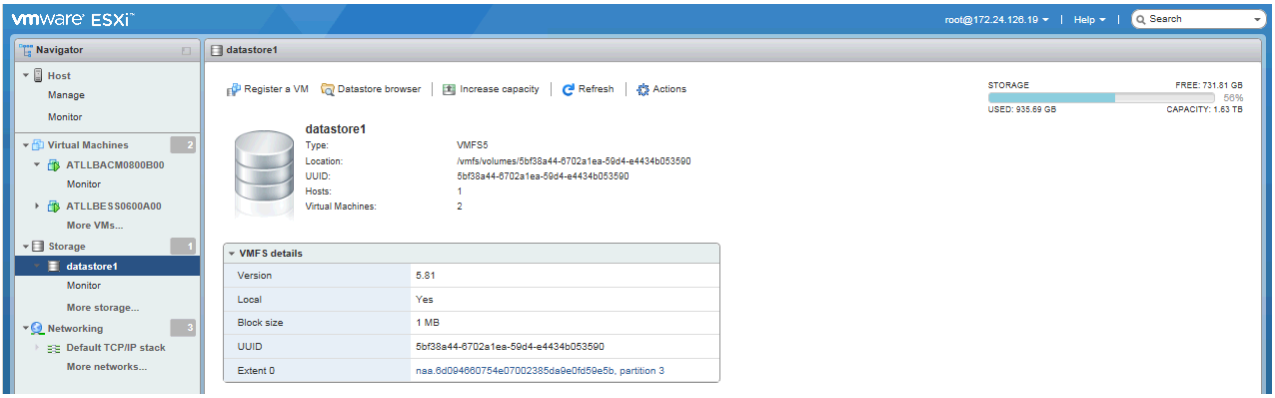
The example in the instructions below is for ESXi 6.5 U2 A07, Build#10719125. This is applicable for all updates. However, the June 2022 update ESXi 6.5 U3 Build#19092475 requires a different update command and that is noted in Steps 13-14. Other than the update command difference, creating a unique directory name relevant for the update, selecting the correct version of the zip file and verifying the correct checksum and ESXi version, the steps are applicable to all versions.

Use the following SHA256 checksum values for the appropriate zip file. All checksums (md5, SHA1, SHA256) are also available on plds.avaya.com in the description of each PLDS download id.

Date	**Dell Customized Version of VMware**	**Zip File Name (for update from previous version)** **PLDS ID** ***SHA256 Checksum***
March 2019	**ESXi 6.5 U2** A07, Build#10719125	VMware-VMvisor-Installer-6.5.0.update02-10719125.x86_64-DellEMC_Customized-A07.zip **PLDS ID:** ACP0000003 SHA256: b2aeb7e6b2356697934640977ba63c71eb41493abd32f8e2af05fc4c755d021d
December 2019	**ESXi 6.5 U2** A12, Build#13635690	VMware-VMvisor-Installer-6.5.0.update02-13635690.x86_64-DellEMC_Customized-A12.zip **PLDS ID:** ACP0000007 SHA256: 3aa0e056f96c01357ef85305221ad62d463ad18c0aa8126e35fd875c660b1612
October 2020	**ESXi 6.5 U3** A05 Build#15256549	VMware-VMvisor-Installer-6.5.0.update03-15256549.x86_64-DellEMC_Customized-A05.zip **PLDS ID:** ACP0000010 SHA256: 6921671f627c8cdeefc6ce498d50edcf2d67e415e4448ad8c2c373c32fd88005
June 2021	**ESXi 6.5 U3** A06 Build#17167537	VMware-VMvisor-Installer-6.5.0.update03-17167537.x86_64-DellEMC_Customized-A06.zip **PLDS ID:** ACP0000013 SHA256: b2140c45bc64cbf428c38709608f1ca833b08a8c1bf5ef4e5785b346359b1f67
October 2021	**ESXi 6.5 U3** A07 Build#17477841	VMware-VMvisor-Installer-6.5.0.update03-17477841.x86_64-DellEMC_Customized-A07.zip **PLDS ID:** ACP0000016 SHA256: ba6276fdd876e9ae76f9a9cb4f2b5179f34f242b295b24b9a8be25a06f771563
June 2022	**ESXi 6.5 U3** Build#19092475	VMware-Dell-Customized-ESXi6.5u3-19092475.zip **PLDS ID:** ACP0000018 SHA256: 4c248751fb327fd0873f0837235cde9b717ae1101e302464e826aee60319d540

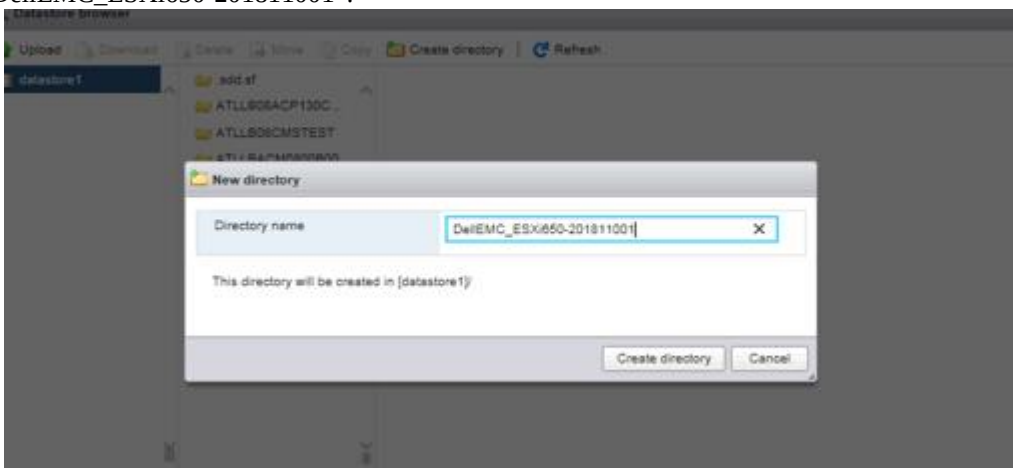
Copy the appropriate zip file to your local PC that will be utilized to access the ESXi Embedded Host Client (EHC) User Interface. In this example that file is “VMware-VMvisor-Installer-6.5.0.update02-10719125.x86_64-DellEMC_Customized-A07.zip”.

1. Login to the ESXi Embedded Host Client (UI) and select “***Storage***”.
2. Select “***datastore1***”.

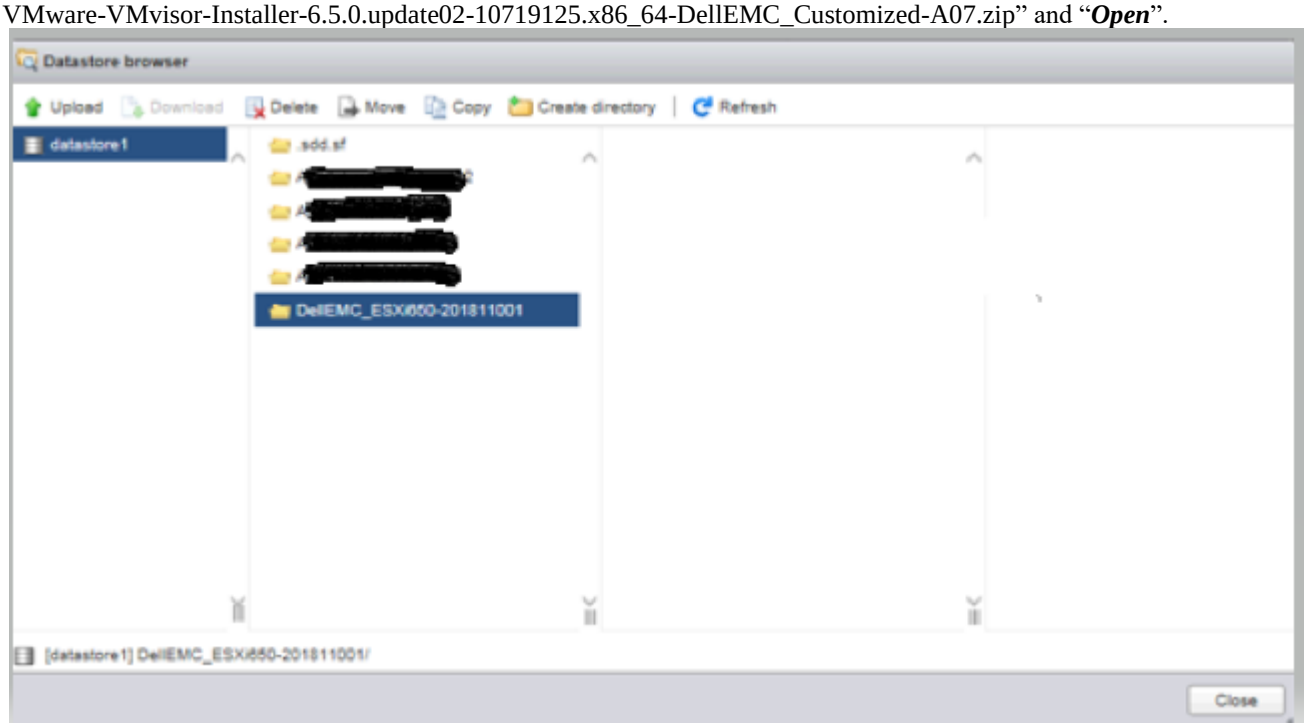


3. Select "***Datastore browser*** ->***Create Directory***".

   Enter a unique Directory Name and then select "***Create directory***". In this example the directory name is "DellEMC_ESXi650-201811001".



4. In the Datastore browser, select the newly created folder and select "***Upload"***. Select the customized zip file. In this example " VMware-VMvisor-Installer-6.5.0.update02-10719125.x86_64-DellEMC_Customized-A07.zip" and "***Open***".



5. The customized zip file should now be uploaded to the directory you created above.

6. Login to the ESXi CLI and navigate to /vmfs/volumes/datastore1/[Directory created above] and verify the sha256sum. Use the corresponding SHA256 checksum from the table above for the zip file you are installing.

```
[root@ACP130DellR640server:~] cd /vmfs/volumes/datastore1
[root@ACP130DellR640server:~] ls -l
drwxr-xr-x    1 root      root           840  Feb   8 08:10  AVAYAACP130SM
drwxr-xr-x    1 root      root          2660 Feb   8 15:33  AVAYAACP130CM
drwxr-xr-x    1 root      root          1120 Feb  10 09:08 AVAYAACP130A
drwxr-xr-x    1 root      root          1120 Feb  10 09:08 AVAYAACP130B
drwxr-xr-x    1 root      root           840 Feb  22 08:08 DellEMC_ESXi650-201811001
[root@ACP130DellR640server:~] cd DellEMC_ESXi650-201811001
[root@ACP130DellR640server:~]  sha256sum VMware-VMvisor-Installer-6.5.0.update02-
10719125.x86_64-DellEMC_Customized-A07.zip
7916e04f476d1d977aada92f8cd7cc0f6f1525cd4aa5149fa12482ff484ea18f  VMware-VMvisor-Installer-
6.5.0.update02-10719125.x86_64-DellEMC_Customized-A07.zip
```

7. On the ESXi Embedded Host Client, select all VMs and perform a guest shutdown.

8. Wait for the VMs to shut down. Click "***Refresh***" to update the display.

9. Place the ESXi host into maintenance mode

10. Login to the ESXi CLI.

11. Verify the date and current vmware version:

```
[root@ACP130DellR640server:~] date && vmware -vl
Mon Mar 19 03:31:33 UTC 2019
VMware ESXi 6.5.0 build-8294253
VMware ESXi 6.5.0 Update 2
```

12. Run the following command to do a pre-check/dry run of the upgrade/updates before install. NOTE DIFFERENT COMMAND REQUIRED for June 2022 update.

Use "esxcli software vib update" for pre-June 2022 updates.

esxcli software vib update -d /vmfs/volumes/[Datastore_Name]/[Directory Name]/[the .zip file] --dry-run

In our example this is:

esxcli software vib update -d /vmfs/volumes/5bf38a44-6702a1ea-59d4-e4434b053590/DellEMC_ESXi650-201811001/VMware-VMvisor-Installer-6.5.0.update02-10719125.x86_64-DellEMC_Customized-A07.zip --dry-run

Verify the dry run output is correct. You should see output similar to the following:

```
Message: Dryrun only, host not changed. The following installers will be applied:
[BootBankInstaller]
Reboot Required: true
VIBS Installed: [long list of VIBs that will be installed]
VIBS Removed: [long list of VIBs that will be removed]
```

Use "esxcli software profile update" for June 2022 updates. If you do not use this command, when logging into the ESXi UI the profile is not updated and shows an older profile name from previous installations/updates.

NOTE: The image profile name may have a different naming convention from the file name. In this example, the image profile has an extra dash that is not present in the file name.

Image profile == *VMware-Dell-Customized-ESXi-6.5u3-19092475*
File name == *VMware-Dell-Customized-ESXi6.5u3-19092475.zip*

esxcli software profile update -p [image profile] -d /vmfs/volumes/[Datastore_Name]/[Directory Name]/[the .zip file] --dry-run

In our example this is:
esxcli software profile update -p VMware-Dell-Customized-ESXi-6.5u3-19092475 -d /vmfs/volumes/5bf38a44-6702a1ea-59d4-e4434b053590/DellEMC_ESXi650-201811001/VMware-Dell-Customized-ESXi6.5u3-19092475.zip --dry-run

Verify the dry run output is correct. You should see output similar to the following:

```
Message: Dryrun only, host not changed. The following installers will be applied: [BootBankInstaller]
Reboot Required: true
VIBS Installed: [long list of VIBs that will be installed]
VIBS Removed: [long list of VIBs that will be removed]
```

13. Now run the same command without the dry run option to install the update:

Use "esxcli software vib update" for pre-June 2022 updates.

esxcli software vib update -d /vmfs/volumes/[Datastore_Name]/[Directory Name]/[the .zip file]

In our example this is:
esxcli software vib update -d /vmfs/volumes/5bf38a44-6702a1ea-59d4-e4434b053590/DellEMC_ESXi650-201811001/VMware-VMvisor-Installer-6.5.0.update02-10719125.x86_64-DellEMC_Customized-A07.zip

Use "esxcli software profile update" for June 2022 updates. If you do not use this command, when logging into the ESXi UI the profile is not updated and shows an older profile name from previous installations/updates.

NOTE: The image profile name may have a different naming convention from the file name. In this example, the image profile has an extra dash that is not present in the file name.
Image profile == *VMware-Dell-Customized-ESXi-6.5u3-19092475*
File name == *VMware-Dell-Customized-ESXi6.5u3-19092475.zip*

esxcli software profile update -p [image profile] -d /vmfs/volumes/[Datastore_Name]/[Directory Name]/[the .zip file]

In our example this is:
esxcli software profile update -p VMware-Dell-Customized-ESXi-6.5u3-19092475 -d /vmfs/volumes/5bf38a44-6702a1ea-59d4-e4434b053590/DellEMC_ESXi650-201811001/ VMware-Dell-Customized-ESXi6.5u3-19092475.zip

14. Reboot the host from the CLI:

```
[root@ACP130DellR640server:~]reboot
```

15. After the reboot, take the ESXi host out of maintenance mode either via the Embedded Host Client or via the ESXi CLI by executing

```
[root@ACP130DellR640server:~]  vim-cmd hostsvc/maintenance_mode_exit
```

16. Verify the updated version info either via the Embedded Host Client or via the ESXi CLI by executing the following. Output will depend on the version used for the update.

ESXi 6.5 U2
A07, Build#10719125
[root@ACP130DellR640server:~] vmware -vl
VMware ESXi 6.5.0 build-10719125
VMware ESXi 6.5.0 Update 2

ESXi 6.5 U2
A12, Build#13635690
[root@ACP130DellR640server:~] vmware -vl
VMware ESXi 6.5.0 build-13635690
VMware ESXi 6.5.0 Update 2

ESXi 6.5 U3
A05 Build#15256549
[root@ACP130DellR640serve:~] vmware -vl
VMware ESXi 6.5.0 build-15256549
VMware ESXi 6.5.0 Update 3

ESXi 6.5 U3
A06 Build#17167537
[root@ACP130DellR640serve:~] vmware -vl
VMware ESXi 6.5.0 build-17167537
VMware ESXi 6.5.0 Update 3

ESXi 6.5 U3
A07 Build#17477841
[root@ACP130DellR640serve:~] vmware -vl
VMware ESXi 6.5.0 build-17477841
VMware ESXi 6.5.0 Update 3

ESXi 6.5 U3
Build#19092475
[root@ACP130DellR640serve:~] vmware -vl
VMware ESXi 6.5.0 build-19092475
VMware ESXi 6.5.0 Update 3

Workaround or alternative remediation

N/A.

Remarks

March 21, 2019: Issue 1.
April 15, 2019: Issue 2 – updated the sha256 sum in step 8 and clarified path in steps 14,15.
December 6, 2019: Issue 3 – new ESXi 6.5 U2 A12 image available.
October 12, 2020: Issue 4 – new ESXi 6.5 U3 A05 update available. Changed ACP reference to ASP.
June 25, 2021: Issue 5 – new ESXi 6.5 U3 A06 update available.
October 27, 2021: Issue 6 – new ESXi 6.5 U3 A07 update available.
October 29, 2021: Issue 7 – clarified in Patch Notes that no rollback is available or supported when updating to new ESXi 6.5 builds.
June 15, 2022: Issue 8 – new ESXi 6.5 U3 build #19092475 update available.
July 21, 2022: Issue 9 – corrected *esxcli software profile update command* – it was missing the "-p" option.
July 25, 2022: Issue 10 – clarified difference between profile name and file name.
October 7, 2022: Issue 11 – Updated to announce VMware ESXi 6.5 End of General Support and requirement to update to ASP 5.1.x.
January 17, 2023: Issue 12—Clarified should update to latest Avaya Solutions Platform R5.1.
March 21, 2024: Issue 13 – Clarified upgrade path to R5.1 as well as historical content of this PSN.

Patch Notes

Backup before applying the patch

Always.

Download

Download the necessary Customized Image of VMware ESXi 6.5 identified in the table above, from plds.avaya.com.

Patch install instructions	Service-interrupting?
As documented in the Resolution Section of this PSN.	Yes

Verification

From the ESXi CLI, execute “vmware -vl”. Output will depend on the version used for the update:

ESXi 6.5 U2; A07, Build#10719125

[root@ACP130DellR640server:~] vmware -vl
VMware ESXi 6.5.0 build-10719125
VMware ESXi 6.5.0 Update 2

ESXi 6.5 U2; A12, Build#13635690

[root@ACP130DellR640server:~] vmware -vl
VMware ESXi 6.5.0 build-13635690
VMware ESXi 6.5.0 Update 2

ESXi 6.5 U3; A05 Build#15256549

[root@ACP130DellR640serve:~] vmware -vl
VMware ESXi 6.5.0 build-15256549
VMware ESXi 6.5.0 Update 3

ESXi 6.5 U3; A06 Build#17167537

[root@ACP130DellR640serve:~] vmware -vl
VMware ESXi 6.5.0 build-17167537
VMware ESXi 6.5.0 Update 3

ESXi 6.5 U3; A07 Build#17477841

[root@ACP130DellR640serve:~] vmware -vl
VMware ESXi 6.5.0 build-17477841
VMware ESXi 6.5.0 Update 3

ESXi 6.5 U3; Build#19092475

[root@ACP130DellR640serve:~] vmware -vl
VMware ESXi 6.5.0 build-19092475
VMware ESXi 6.5.0 Update 3

Failure

Contact Avaya Services.

Patch uninstall instructions

No rollback is available or supported when updating to new ESXi 6.5 builds. Return to a previous version of ESXi will require redeployment of ESXi and the VMs.

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

The following utilizes the Common Vulnerability Scoring System version 3 (CVSSv3) base score and metrics as reported by the vendor for the affected component(s) or by the National Institute of Standards and Technology in the National Vulnerability Database. For more information on CVSS and how the score is calculated, see Common Vulnerability Scoring System v3.0: Specification Document

Not all security updates are listed below – these reflect escalations into the Product House. Please reference the Dell Release Notes listed in the Problem Description section of this PSN. They will have links to the VMware Release Notes for further information.

ESXi 6.5 U3, Build#19092475

VMware Security Advisory ID	Severity	Vulnerability	CVSSv3 Base Score	CVSSv3 Metrics
VMSA-2022-0004	Important	CVE-2021-22040, CVE-2021-22041	8.4 (High) 8.4 (High)	CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

VMSA-2022-0001 (delivered in ESXi 6.5 build 18678235)	Important	CVE-2021-22045	7.7 (High)	CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

ESXi 6.5 U3, A07

VMware Security Advisory ID	Severity	Vulnerability	CVSSv3 Base Score	CVSSv3 Metrics
VMSA-2021-0002	Critical	CVE-2021-21972, CVE-2021-21973, CVE-2021-21974	9.8 (Crit) 5.3 (Med) 8.8 (High)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

ESXi 6.5 U3, A06

VMware Security Advisory ID	Severity	Vulnerability	CVSSv3 Base Score	CVSSv3 Metrics
VMSA-2020-0026	Critical	CVE-2020-4004, CVE-2020-4005	8.2 (High) 7.8 (High)	CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

ESXi 6.5 U3, A05

VMware Security Advisory ID	Severity	Vulnerability	CVSSv3 Base Score	CVSSv3 Metrics
VMSA-2019-0005	Critical	CVE-2019-5514, CVE-2019-5515, CVE-2019-5518, CVE-2019-5519, CVE-2019-5524	8.8 (High) 8.8 (High) 6.8 (Med) 6.8 (Med) 8.8 (High)	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
VMSA-2019-0013	Important	CVE-2017-16544, CVE-2019-5531, CVE-2019-5532, CVE-2019-5534	8.8 (High) 5.4 (Med) 7.7 (High) 7.7 (High)	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N
VMSA-2019-0022	Critical	CVE-2019-5544	9.8 (Crit)	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

ESXi 6.5 U2, A12

VMware Security Advisory ID	Severity	Vulnerability	CVSSv3 Base Score	CVSSv3 Metrics
VMSA-2019-0008	Important	CVE-2018-12126	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
		CVE-2018-12127	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
		CVE-2018-12130	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N
		CVE-2019-11091	5.6 (Medium)	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:N/A:N

ESXi 6.5 U2, A07

VMware Security Advisory ID	Severity	Vulnerability	CVSSv3 Base Score	CVSSv3 Metrics
VMSA-2018-0027	Critical	CVE-2018-6981	8.8 (High)	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
		CVE-2018-6982	6.5 (Medium)	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

.

Avaya Security Vulnerability Classification

N/A.

Mitigation

Apply update specified in this PSN.

For additional support, contact your Authorized Service Provider. Depending on your coverage entitlements, additional support may incur charges. Support is provided per your warranty or service contract terms unless otherwise specified.

Avaya Support Contact	Telephone
U.S. Remote Technical Services – Enterprise	800-242-2121
U.S. Remote Technical Services – Small Medium Enterprise	800-628-2888
U.S. Remote Technical Services – BusinessPartners for Enterprise Product	877-295-0099
BusinessPartners for Small Medium Product	Please contact your distributor.
Canada	800-387-4268
Caribbean and Latin America	786-331-0860
Europe, Middle East, and Africa	36-1238-8334
Asia Pacific	65-6872-8686