

[Click Here](#)



Vmware 6. 7 patches

Vmware 6.7 patches. Vmware 6.5 patches. Vmware patch release. Vmware latest patches. Vmware patches download.

****Update Description**** This update resolves four security vulnerabilities (CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, and CVE-2024-22255) in VMware products. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2024-0006. ****Affected Components**** This update affects the following components: * ESXi-6.7.0-20240304001-standard * ESXi-6.7.0-20240304001-no-tools ****Affected VIBs**** The update affects the following VIBs (Virtual Hardware Component): * VMware_bootbank_esx-update 6.7.0-3.193.23084122 * VMware_bootbank_esx-base 6.7.0-3.193.23084122 * VMware_bootbank_vsanhealth 6.7.0-3.193.22695748 * VMware_bootbank_vsan 6.7.0-3.193.22695747 * VMW_bootbank_xhci-xhci 1.0-3vmw.670.3.193.23084122 ****Known Issues from Prior Releases**** The update addresses several known issues, including: * CLI Issues: + Views might switch from the appliance shell to the Direct Console User Interface during an upgrade of the vCenter Server Appliance by using the CLI installer. + vSAN Issues: + PR 2855671: vSAN disk format upgrade fails, objects not upgrading to version 3 * Internationalization Issues: + A VMkernel network using an NSX logical switch might fail for stateless hosts if you register vCenter Server with non-ASCII characters on VMware NSX Manager. ****NSX Manager, ESXi Host, and VDS Name Requirements**** When deploying a stateless host with a VMkernel network using an NSX logical switch, ensure that the vCenter Server is registered to the NSX Manager with a password containing only ASCII characters. This prevents potential loss of network settings. For naming a VDS in a hyper-converged infrastructure (HCI) cluster: - Avoid using strings exceeding 40 characters from extended ASCII codes between 128 and 255 or more than 26 non-ASCII characters. - If the name exceeds these limits, ESXi hosts might stop responding when attempting to add the VDS to a physical adapter. ****OVF Tool Issues**** The OVF Tool may fail to verify an SSL thumbprint if set using CLI. To resolve this: - In DCUI, specify the thumbprint in ssl_certificate_verification or set verification_mode to False for ignoring certificate thumbprints. - Alternatively, use the command-line parameter --no-ssl-certificate-verification. ****Installation and Upgrade Issues**** After updating to ESXi 670-202210001: - Ignore errors related to failed VIB signature verification due to expired signing keys. Refer to VMware knowledge base article 76276 for more information. - For HPE ProLiant - DL380/360 Gen 9 Servers, set the server BIOS mode to UEFI before installing or upgrading ESXi. ****ESXi Rollback Issues**** After rolling back from ESXi version 6.7 to 6.5 or earlier: - Fix compatibility issues with error messages during patch installation and VMware Tools upgrade by running a specific command on the host via SSH. When installing software on an ESXi host, ensure that the vib and zip files match the currently running ESXi version. Note that for VMs already using new VMware Tools, there's no need to revert them when rolling back the ESXi host. Special characters in passwords can cause installation issues. If special characters like backslashes or double-quotes are used in ESXi, vCenter Single Sign-On, or operating system password fields during vCenter Server Appliance Installation templates, the pre-check fails with an error message. To work around this, escape special characters by doubling them up. The Windows vCenter Server 6.7 installer may fail if non-ASCII characters are present in passwords for Chinese, Japanese, Korean, and Taiwanese locales. Ensure that these passwords only contain ASCII characters. If your vCenter Server system is installed on an external database, the user and password must not include non-ASCII characters for certain locales. Additionally, avoid using the colon character (:) as part of the vCenter Server root password when setting up the vSphere Appliance Management Interface. Finally, do not use the backslash character (\) in the vCenter Single Sign-On password during the vCenter Server Appliance UI installer setup. Scripted ESXi installations on HP ProLiant Gen 9 Servers may fail due to an error when multiple USB drives are used during installation and the Embedded User Partition option is enabled in the BIOS. Message partitions not initialized. To work around this issue, disable the Embedded User Partition option in the server BIOS. If you're using a USB drive that's not formatted, remove it from the server or format it with a file system. When upgrading vCenter Server 6.5 for Windows to 6.7, ensure that the vSphere Authentication Proxy service is inactive. If it's active, stop the service before performing the upgrade. You can restart the service after the successful upgrade. Additionally, when patching to vCenter Server 6.7 Update 1 from earlier versions, you might encounter issues if vCenter Server High Availability is enabled. To resolve this, disable vCenter Server High Availability and delete any passive or witness nodes. After the upgrade, recreate your vCenter Server High Availability clusters. When upgrading Windows vCenter Server 6.0.x or 6.5.x to 6.7, ensure that host profiles do not contain non-ASCII or high-ASCII characters. If they do, upgrade the ESXi hosts with these profiles to version 6.0.x or 6.5.x and then update the host profiles. Finally, when upgrading vCenter Server Appliance 6.5 Update 2 and later using custom HTTP and HTTPS ports, you might encounter issues. Unfortunately, there is no workaround for this issue. When converging an external Platform Services Controller to a vCenter Server, ensure that the Platform Services Controller uses the default HTTPS port (443) before running the vCenter External to Embedded Convergence tool. Upgrading to vCenter Server 6.7 Update 2 may cause issues with FCDs in the Global Catalog. During a system upgrade, the FCD Global Catalog might select an ESXi host not yet updated and fail synchronization. This may lead to incomplete results from the VStorageObjectForSpec API for previously created FCDs prior to the upgrade. Workaround: Ensure all ESXi hosts are upgraded before starting syncDatastore API with fullSync set to true. Editing the etc/issue file during appliance upgrades using Virtual Appliance Management Infrastructure fails if the text is not split into new lines. An error message will appear indicating unexpected content in the etc/issue file. Workaround: Restore the contents of the etc/issue file before an upgrade using Virtual Appliance Management Interface. Upgrades to vCenter Server 6.7 Update 3l and later may cause existing or new HPE VASA providers to be in a disconnected state, especially for supported virtual volumes on 3PAR StoreServ or Primera. However, this issue is not present in 3PAR 3.3.1 MU3 storage. Workaround: Upgrade to vCenter Server 7.0 Update 1c and later. Alternatively, you can restore your system to a backup prior to vCenter Server 6.7 Update 3l or postpone the VASA provider upgrade until HPE resolves the issue. Running the camregister command with the -x option fails when the vCenter Single Sign-On password packet loss for a few seconds during upgrade. Workaround: Upgrade switches sequentially; schedule upgrade during maintenance window; set DRS mode to manual and don't apply recommendations. VM fails to power on when Network I/O Control is enabled and all active uplinks are down due to distributed port group teaming policy and standby adapter reservation. Workaround: Move available standby adapters to active adapters list in teaming policy of distributed port group. Network flapping on NIC with qle3f driver might cause ESXi host to crash (PSOD). Some physical NICs might experience issues: ****Link status flapping****: A qle3f driver issue causes frequent link status changes every 1-2 seconds. Workaround: Ensure network stability and avoid link status fluctuations. ****Packet recognition failure****: ERSPAN Type III packets may not be recognized by packet analyzers due to incorrect header bits. Workaround: Use GRE or ERSPAN Type II packets instead, if supported. ****vDNS configuration limitations****: esxcli commands for DNS configuration are not supported on non-default TCP/IP stacks. Workaround: Avoid using these commands on non-default stacks. ****Host profile error****: A compliance check fails when applying a host profile with an enabled default IPv4 gateway for vmknic interface. Workaround: Edit the host profile settings and select a valid default IPv4 gateway. Additionally, Intel Fortville series NICs have limitations: ****Geneve encapsulation issues****: These NICs cannot receive Geneve encapsulation packets with option lengths bigger than 255 bytes. Workaround: Disable hardware VLAN stripping to resolve this issue. RSPAN SRC mirror sessions may also fail after migration: ****Mirror session failure****: When a VM connected to an RSPAN SRC mirror session is migrated, and there's no required pNIC on the destination network, the mirror session fails to configure. Workaround: Remove and re-add the failed port or disable and re-enable it. Storage issues may occur: ****NFS datastore read-only issue****: A host's NFS datastores may become read-only due to a temporary loss of IP address or after a stateless hosts reboot. Workaround: Unmount and remount the datastores, or set write permission for both the NFS vmknic and management vmknic. Lastly: ****VM storage policy failure****: Selecting Host-local PMem Storage Policy in the Edit VM Storage Policies dialog may fail with an error. You cannot apply Host-local PMem Storage Policy to VM home due to compatibility issues. However, you can use the migration wizard to migrate virtual disks and then apply this policy. Permanent device loss state in ESXi hosts might cause inaccessible datastores even after recovery. To resolve this, perform a Rescan Storage operation from vCenter Server on affected hosts. When working with non-vSAN datastores, backingObjectID and SnapshotInfo fields for First Class Disks are always set to null. In contrast, vSAN datastores populate these fields when creating snapshots of First Class Disks. However, updating snapshot information does not change after deleting older snapshots. Migrating a virtual machine from VMFS3 to VMFS5 is unsuccessful in mixed ESXi host environments (6.5 and 6.7). The solution is to upgrade the VMFS3 datastore to VMFS5 for successful migration. After upgrading a failed-to-upgrade VMFS3 datastore using CLI, it might still report errors. This is due to the ongoing detection of the VMFS3 volume by the host, which reports deprecated volumes that need upgrading to VMFS5 for continued availability on vSphere 6.7 hosts. To remove this error message, restart the hostd service or reboot the host. There could be performance degradation in drivers using Default Queue Receive Side Scaling (DRSS) when the DRSS feature is enabled, impacting network traffic distribution and CPU processing efficiency. Native software FCoE adapters configured on an ESXi host might disappear when the host is rebooted. To recover the vmkfcoe adapter: Run "esxcli storage core adapter list" to confirm its absence, then verify vSwitch configuration on associated vmknic. Discover FCoE vmbas with "esxcli fcoe nic discover -v vmnic_number". Attempts to create a VMFS datastore on an ESXi 6.7 host might fail in certain software FCoE environments. Configurations include native software FCoE adapters and Cavium QLogic 57810/40 CNAs connected directly to a Dell EMC VNX5300 or VNX5700 series storage array's FCoE port via Cisco FCoE switch. Workaround: Switch to ESXi host > Cisco FCoE switch > FC switch > storage array configuration. Performance degradation might occur with DRSS enabled on Mellanox adapter cards; disable it if necessary using "esxcli system module parameters set" command, then reboot the host. When extracting a host profile, the Datastore name field is empty in the CoreDump File setting of the host profile; edit host profile settings to select Create the coredump file with an explicit datastore and size option. Native software FCoE adapters might disappear on reboot after enabling them with vmkfcoe driver; perform steps: "esxcli storage core adapter list" verification, vSwitch configuration check, and adapter discovery using "esxcli fcoe nic discover -v vmnic_number". Backup unicode files display differently in Windows Explorer than in browsers or file system paths. Workaround: Access backups through your web browser instead of Windows Explorer. Successfully upgrading to vCenter Server Appliance 6.7 requires logging in with the root password set during deployment at . In the vCenter Server Appliance Management Interface, clicking Time and then Edit in the Time Synchronization pane enables disabling NTP time synchronization, instead relying on system time zone settings. Logging into the vSphere Web Client with Windows session authentication fails for Firefox browsers version 54 or later. To resolve this, use an alternative browser like Internet Explorer, Chrome, or Firefox version 53 and earlier. Hardware health alarm notifications do not trigger in some instances when multiple sensors on an ESXi host are tripped within a short time span. As a result, traps and email notifications may not be sent. Checking the hardware sensors section for any alerts is recommended. The vSphere Client and vSphere Web Client might not reflect updates from vCenter Server 6.7 to 6.7 Update 1 for vCenter Server for Windows. Therefore, the build number details for vpxd in these clients may show version 6.7.0 instead of 6.7.0. When using the VCSA Installer Time Sync option, it is essential to connect the target ESXi to an NTP server in the Time & Date Setting from the ESX Management. Failure to do so during installation results in a failed configuration. Monitoring Windows vCenter Server health may display an error message indicating that the Health service is not available for Windows vCenter Server. However, this issue can be ignored, and users can access vSAN health information through the vCenter Server Appliance. Hardware health alarms do not function with earlier ESXi versions such as 6.5 Update 1 or earlier when added to vCenter 6.7. Some cases may cause vCenter Server to stop working when using vmodl to edit or expand a disk. This issue can occur even with an earlier vmodl. No workaround is available. Migrating vCenter Server for Windows 6.0.x or 6.5.x to vCenter Server Appliance 6.7 may fail during the data export stage with an error message: "The compressed zip folder is invalid or corrupted." To resolve this, you must manually create a zip file from the export data and set an environment variable MA_INTERACTIVE_MODE before starting the migration. In some cases, there might be a discrepancy between the build number displayed in VAMI and the vSphere Client. No workaround is available for this issue. vCenter Server Appliance 6.7 may display an error message in the Available Update section of the vCenter Server Appliance Management Interface (VAMI). This issue will be resolved with the release of the first patch for vSphere 6.7, but no workaround is needed as it does not impact functionality. When a datastore becomes inaccessible and enters the All Paths Down state, the name of a virtual machine in the inventory may change to its path name. After resolving the storage issue, the virtual machine's name will be displayed again. To enable VBS (Virtualization-Based Security) for an AMD-based guest OS, you must select the "Secure boot" Platform Security Level when enabling VBS. Virtualization Based Security (VBS) is a feature in Windows 10 and Windows Server 2016, supported by vSphere since version 6.7. However, it has some limitations: ****Memory and CPU Hot Addition****: Enabling VBS within Windows prevents hot adding memory or CPU for Windows VMs. - Workaround: Power off the VM, change memory or CPU settings, then power on the VM. ****Linked Clone VM Incompleteness****: After a vSAN network recovery from failure, the snapshot tree of a linked-clone VM might be incomplete. This is due to the hostd service not detecting that the parent VM namespace has regained accessibility. - Workaround: Unregister and then re-register the VM to force hostd to reload the VM state. Additionally: ****Virtual Appliance Management Interface Display Issues****: During patching from vCenter Server 6.7 to later versions, calls from the interface might fail to reach the back end applmgmt service. - Workaround: Refresh the browser and log in again after a complete appliance backend reboot. ****Wizard Rendering Issue****: The Ready to Complete page of the Register Virtual Machine wizard might display only one horizontal line due to rendering issues. However, this does not affect the workflow of the wizard. Lastly: ****VMware Service Lifecycle Manager Restart Issues****: Enabling Storage I/O Control for a large number of connected ESXi hosts can cause vpxd service restarts. - Workaround: Disable Storage I/O Control or reduce the number of connected hosts to prevent this issue. When configuring Proactive HA in Manual/MixedMode in vSphere 6.7 RC build, you might encounter two prompts to apply DRS recommendations. The first prompt asks for entering the host into maintenance mode, and the second prompt requires migrating all VMs on that host. For lazy import upgrade workflows without VCHA configuration, there's no interaction with VCHA. However, setting up a fresh VCHA while lazy import is in progress can lead to performance issues due to large data cloning requirements. Adding ESXi hosts running vSphere Fault Tolerance workloads to a vCenter Server system using the vSphere Client might fail with an error message. Instead, consider scheduling a task to add the host or use the vSphere Web Client for this operation. Configuring vCenter Server High Availability clusters by using an NSX-T logical switch might also result in failure due to connection issues. Workarounds include configuring HA clusters via a vSphere Distributed Switch instead. Lastly, during ESXi stateless host reboots provisioned with vSphere Auto Deploy, the numRxQueue value is lost and needs to be reset manually after each reboot. When booting from cache in UEFI mode, you need to explicitly select the device from the UEFI boot manager for the process to succeed. In Stateless Caching, a reboot might fail if the autodeploy service is down and the ESXi image cannot be found on the disk. The workaround is to manually select the disk with the cached image in the UEFI Boot Manager. Using UEFI firmware with VMware vSphere Auto Deploy can cause issues when deploying an ESXi image over a VLAN network. This is due to the implementation of VLAN support by some UEFI firmware vendors, which might not fully support iPXE. There is no workaround for this issue. Stateless ESXi hosts may take up to 20 minutes or more to boot with 1,000 configured datastores. Currently, there is no workaround for this issue. When adding or editing ESXi users through the VMware Host Client, you will see the option to enable shell access. However, this only works for users with full access admin permissions, and there is no workaround for this issue. ESXi hosts may fail with a purple diagnostic screen and a #PF Exception 14 error when using the qle3f driver. This can occur when losing FCoE connections or unloading the driver. There is no workaround for this issue. Rebooting ESXi hosts with VMs running on iSCSI LUNs claimed by the qle3i driver can cause failure. The workaround is to power off VMs before rebooting the host. VXLAN stateless hardware offloads are not supported when using Guest OS TCP traffic over IPv6 on Cisco UCS VIC 13xx adapters. This can cause traffic disruption and incorrect packet checksums, leading to issues with ESXi software stack. There is no workaround for this issue. Incorrect TCP protocol processing in Guest OS, causing issues. To resolve this issue, disable VXLAN stateless offload feature for VXLAN encapsulated TCP traffic over IPv6 on Cisco UCS VIC 13xx adapters. Disable the Virtual Extensible LAN field in Ethernet Adapter Policy to achieve this. Alternatively, uncheck Enable VXLAN field in Ethernet Interfaces vNIC properties section on a Cisco C-Series UCS server. ESXi provides batch QueryUnresolvedVnfsVolume API to query and list unresolved VMFS volumes or LUN snapshots. To decrease query operation time, disable filesystem liveness check by adding parameter FALSE in hostd configuration file. Additionally, importing .csv file during host customization overwrites user input. The vCenter Server Convergence Tool might fail to convert an external Platform Services Controller due to conflicting IP and FQDN settings. Clean up stale service ID entry before proceeding with restore process as mentioned in VMware knowledge base article 2131327. vCenter Server 6.7 might display credentials validation errors, causing login issues after upgrade. After upgrading to vCenter Server 6.7, attempting to log in using the vSphere Web Client or vSphere Client with a security token or smartcard may result in an error message unable to validate submitted credentials. To resolve this issue, try removing and re-adding the identity source. For more information, refer to Adding or Editing a vCenter Single Sign-On Identity Source. Reverting an ESXi host to an older version can introduce new CPU IDs like IBPB into an Enhanced vMotion Compatibility (EVC) cluster, even if the host lacks these features. This issue is resolved in this release, but removing unqualified hosts from EVC clusters may be necessary. Some vCenter Server plug-ins may not render the dark theme mode correctly in the vSphere Client after changing color schemes. Enabling per-VM EVC can cause virtual machines to fail power on if VMware vCenter Server 6.7 Update 1 is installed or upgraded but ESXi 6.7 Update 1 is not applied, particularly on unpatched hosts with EVC enabled at the cluster level. When using a machine with an NVDIMM of less than 16MB, you might encounter issues during the initialization of a new disk. In some cases, this could result in a blue diagnostic screen or an error message in the Disk Management window. A possible workaround is to increase the size of the virtual NVDIMM to 16MB or larger. Another issue may occur when installing ESXi on hosts with hardware iSCSI disks connected to Emulex OneConnect OCe11100 or 14000 NIC devices. This could cause the hostd service to fail, preventing stateful installation. A workaround is to install a vendor-provided async version of the elx-esx-libelsina plug-in. You might also experience intermittent issues with the ESXi SNMP service stopping work. If your environment has IPv6 disabled, this issue may occur. In such cases, you can manually restart the SNMP service or use a cron job to periodically restart it. Furthermore, the sensor daemon might fail to report ESXi host hardware status due to a logic error in IPMI SDR validation. This could result in no output when running the command vsish -e get /power/hostStats. There is currently no known workaround for this issue. Additionally, after upgrading to ESXi 6.7, networking workloads on Intel 10GbE NICs may cause higher CPU utilization under certain conditions. A possible workaround is to revert back to the legacy VMKLinux ixgbe driver. Finally, initial installation of DELL CIM VIB might fail to respond. A workaround for this issue is to enter two commands to restart sfcdb: esxcli system wbem set --enable false and then esxcli system wbem set --enable true. ****ESXi Image Profiles: A Series of Updates**** The latest image profile for ESXi, ESXi-6.7.0-20221004001-standard (Build 20497097), was released in October 2022 and includes updated VIBs. This is part of a series of updates that have been made to the platform since November 2018. ****Key Updates**** Here are some key updates in the ESXi image profiles: ****ESXi-6.7.0-20221004001-standard (Build 20497097)****: Released in October 2022, this update includes updated VIBs and can be found on the official documentation website. ****ESXi-6.7.0-20220704001-standard (Build 19997733)****: Released in July 2022, this update included updated VIBs and was part of a larger series of updates to the platform. ****ESXi-6.7.0-20210304001-standard (Build 17700523)****: Released in March 2021, this update marked a significant milestone for ESXi, with updated VIBs and improved performance. ****Release Notes**** For more information on each of these updates, including detailed release notes and instructions for installation, please visit the official documentation website. The provided text outlines various ESXi-6.7.0 image profiles, each with its corresponding build number and updated VIBs (Virtual Infrastructure Bundles). The following dates are mentioned: December 5, 2019; November 12, 2019; August 20, 2019; June 20, 2019; May 14, 2019; April 30, 2019; April 11, 2019; March 28, 2019; January 17, 2019; November 9, 2018; October 16, 2018; and other dates. The text includes information on the release notes for each build.