

VMware ESXi670-202210001Release Notes

Release Date: 06 October, 2022

What's in the Release Notes

The release notes cover the following topics:

- [Patch Build Details](#)
- [Resolved Issues](#)
- [Known Issues](#)

Build Details

Download Filename:	ESXi670-202210001.zip
Build:	20497097
Download Size:	465.1 MB
md5sum:	ce070930b9f8c600d1b36c2173d54fc4
sha256checksum:	b59cc0837acb7e50037dd353da5981969d5cf2fee8367e8a30781d5541164eb1
Host Reboot Required:	Yes
Virtual Machine Migration or Shutdown Required:	Yes

Bulletins

Bulletin ID	Category	Severity
ESXi670-202210401-BG	Bugfix	Important
ESXi670-202210402-BG	Bugfix	Important
ESXi670-202210403-BG	Bugfix	Important
ESXi670-202210101-SG	Security	Important
ESXi670-202210102-SG	Security	Important
ESXi670-202210103-SG	Security	Important
ESXi670-202210104-SG	Security	Important

Rollup Bulletin

This rollup bulletin contains the latest VIBs with all the fixes since the initial release of ESXi 6.7.

Bulletin ID	Category	Severity
ESXi670-202210001	Bugfix	Important

IMPORTANT: For clusters using VMware vSAN, you must first upgrade the vCenter Server system. Upgrading only the ESXi hosts is not supported. Before an upgrade, always verify in the [VMware Product Interoperability Matrix](#) compatible upgrade paths from earlier versions of ESXi, vCenter Server and vSAN to the current version.

Image Profiles

VMware patch and update releases contain general and critical image profiles. Application of the general release image profile applies to new bug fixes.

Image Profile Name
ESXi-6.7.0-20221004001-standard
ESXi-6.7.0-20221004001-no-tools
ESXi-6.7.0-20221001001s-standard
ESXi-6.7.0-20221001001s-no-tools

For more information about the individual bulletins, see the [Product Patches](#) page and the [Resolved Issues](#) section.

Patch Download and Installation

The typical way to apply patches to ESXi hosts is by using the VMware vSphere Update Manager. For details, see the [About Installing and Administering VMware vSphere Update Manager](#).

ESXi hosts can be updated by manually downloading the patch ZIP file from [VMware Customer Connect](#). From the **Select a Product** drop-down menu, select **ESXi (Embedded and Installable)** and from the **Select a Version** drop-down menu, select **6.7.0**. Install VIBs by using the `esxcli software vib update` command. Additionally, you can update the system by using the image profile and the `esxcli software profile update` command.

For more information, see the [vSphere Command-Line Interface Concepts and Examples](#) and the [vSphere Upgrade Guide](#).

Resolved Issues

The resolved issues are grouped as follows.

- [ESXi670-202210401-BG](#)
- [ESXi670-202210402-BG](#)
- [ESXi670-202210403-BG](#)
- [ESXi670-202210101-SG](#)
- [ESXi670-202210102-SG](#)
- [ESXi670-202210103-SG](#)
- [ESXi670-202210104-SG](#)
- [ESXi-6.7.0-20221004001-standard](#)
- [ESXi-6.7.0-20221004001-no-tools](#)
- [ESXi-6.7.0-20221001001s-standard](#)
- [ESXi-6.7.0-20221001001s-no-tools](#)

ESXi670-202210401-BG

Patch Category	Bugfix
Patch Severity	Important
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	<ul style="list-style-type: none">• VMware_bootbank_esx-update_6.7.0-3.189.20497097• VMware_bootbank_vsanhealth_6.7.0-3.189.20235860• VMware_bootbank_esx-base_6.7.0-3.189.20497097• VMware_bootbank_vsan_6.7.0-3.189.20235859
PRs Fixed	2945696, 2960623, 2977958, 2994957, 3001186, 3012635
CVE numbers	N/A

Updates [esx-base](#), [esx-update](#), [vsan](#), and [vsanhealth](#) VIBs to resolve the following issues:

- - **PR 3012635: After creating or reverting to a VM snapshot, VMware Tools guest-related performance counters stop to update**

Rarely, due to the fast suspend resume mechanism used to create or revert a VM to a snapshot, the internal state of the VMX process might reinitialize without notification to the upper layers of the virtual infrastructure management stack. As a result, all guest-related performance counters that VMware Tools provides stop updating. In all interfaces to the ESXi host, you continuously see the last recorded values.

This issue is resolved in this release.
 - **PR 3001186: VM events sometimes report the template property incorrectly**

In rare cases, VM events might report the `template` property, which indicates if a virtual machine is marked as a template, incorrectly. As a result, you might see the `template` property as `true` even if the VM is not a template VM or as `false`, when a VM is marked as a template.

This issue is resolved in this release.
 - **PR 2945696: You might see outdated path states to ALUA devices on an ESXi host**

In an ALUA target, if the target port group IDs (TPGIDs) are changed for a LUN, the cached device identification response that SATP uses might not update accordingly. As a result, ESXi might not reflect the correct path states for the corresponding device.

This issue is resolved in this release.
 - **PR 2960623: You cannot migrate virtual machines with raw device mapping (RDM) disks due to a mismatch in the LUN VML IDs between ESXi hosts**

Migrating virtual machines with RDM disks by using vSphere Storage vMotion might fail due to a mismatch of the VML IDs that identify the storage devices on the ESXi hosts in a cluster.

This issue is resolved in this release. The fix makes sure that if VML IDs for the same LUN are different in two ESXi hosts, ESXi uses a mask for the `dd` bytes that represent the LUN numbers before using the VML IDs to compare devices. For more information on VML IDs, see VMware knowledge base article [2078730](#).
 - **PR 2994957: You do not see memory status info for ESXi hosts in the Managed Object Browser (MOB) interface**

Due to a missing Memory Module Entity for Cisco servers in the Managed Object Browser, you might not see the memory status info of an ESXi host by using MOB.

This issue is resolved in this release. The fix adds support for Memory Module Entity ID 8 (08h).
 - **PR 3000194: Virtual machines might become unresponsive after a cross-host Storage vMotion operation failure due to a timeout**

Due to a possible timeout of I/O requests during a cross-host Storage vMotion operation, the migration task might fail and as a result, some virtual machines become unresponsive.

This issue is resolved in this release.

- **PR 2984140: If a virtual machine reboots while a snapshot is deleted, the VM might fail with a core dump**

If a running virtual machine reboots during a snapshot deletion operation, the VM disks might be incorrectly reopened and closed during the snapshot consolidation. As a result, the VM might fail. However, this is a timing issue and occurs accidentally.

This issue is resolved in this release.

ESXi670-202210402-BG

Patch Category	Bugfix
Patch Severity	Important
Host Reboot Required	No
Virtual Machine Migration or Shutdown Required	No
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	<ul style="list-style-type: none">• VMware_bootbank_esx-xserver_6.7.0-3.189.20497097
PRs Fixed	N/A
CVE numbers	N/A

Updates the **esx-xserver** VIB.

ESXi670-202210403-BG

Patch Category	Bugfix
Patch Severity	Important
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	<ul style="list-style-type: none">• VMW_bootbank_ntg3_4.1.8.0-4vmw.670.3.189.20497097
PRs Fixed	2992533
CVE numbers	N/A

Updates the **ntg3** VIB to resolve the following issue:

- **PR 2992533: You see link flapping on NICs that use the ntg3 driver of version 4.1.3 and later**

When two NICs that use the **ntg3** driver of versions 4.1.3 and later are connected directly, not to a physical switch port, link flapping might occur. The issue does not occur on **ntg3** drivers of versions earlier than 4.1.3 or the **tg3** driver. This issue is not related to the occasional Energy Efficient Ethernet (EEE) link flapping on such NICs. The fix for the EEE issue is to use an **ntg3** driver of version 4.1.7 or later, or disable EEE on physical switch ports.

This issue is resolved in this release. ESXi670-202210001 comes with **ntg3** driver version 4.1.8. However, after you upgrade the **ntg3** driver to version 4.1.8, you must set the new module parameter **noPhyStateSet** to **1**. The **noPhyStateSet** parameter defaults to **0** and is not required in most environments, except they face the issue.

ESXi670-202210101-SG

Patch Category	Security
Patch Severity	Important
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	<ul style="list-style-type: none">• VMware_bootbank_esx-base_6.7.0-3.185.20491463• VMware_bootbank_esx-update_6.7.0-3.185.20491463• VMware_bootbank_vsan_6.7.0-3.185.20179805• VMware_bootbank_vsanhealth_6.7.0-3.185.20179806
PRs Fixed	2994841, 2994849, 2994852, 2994853, 3001982, 3015508

CVE numbers	N/A
-------------	-----

Updates [esx-base](#), [esx-update](#), [vsan](#), and [vsanhealth](#) VIBs to resolve the following issues:

- ESXi670-202210001 provides the following security updates:
 - cURL is updated to version 7.84.0.
 - The OpenSSL library is updated to versions 1.0.2zf.
 - The SQLite database is updated to version 3.39.0.
 - The tcpdump package is updated to version 4.9.1.
 - This release resolves CVE-2022-31681. For more information on this vulnerability and its impact on VMware products, see [VMSA-2022-0025](#).
 - This release resolves CVE-2018-5733. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of [7.5](#).

ESXi670-202210102-SG

Patch Category	Security
Patch Severity	Important
Host Reboot Required	No
Virtual Machine Migration or Shutdown Required	No
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	<ul style="list-style-type: none"> VMware_bootbank_esx-ui_1.43.10-20199807
PRs Fixed	N/A
CVE numbers	N/A

Updates the [esx-ui](#) VIB.

ESXi670-202210103-SG

Patch Category	Security
Patch Severity	Important
Host Reboot Required	No
Virtual Machine Migration or Shutdown Required	No
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	<ul style="list-style-type: none"> VMware_locker_tools-light_12.0.6.20104755-20491463
PRs Fixed	3015657
CVE numbers	N/A

Updates the [tools-light](#) VIB to resolve the following issue:

- The following VMware Tools ISO images are bundled with ESXi 670-202210001:
 - [windows.iso](#): VMware Tools 12.0.6 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
 - [linux.iso](#): VMware Tools 10.3.24 ISO image for Linux OS with glibc 2.11 or later.

The following VMware Tools ISO images are available for download:

- VMware Tools 11.0.6:
 - [windows.iso](#): for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).
 - VMware Tools 10.0.12:
 - [winPreVista.iso](#): for Windows 2000, Windows XP, and Windows 2003.
 - [linuxPreGLibc25.iso](#): supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with glibc version earlier than 2.5.
 - [solaris.iso](#): VMware Tools image 10.3.10 for Solaris.
 - [darwin.iso](#): Supports Mac OS X versions 10.11 and later.

Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:

- [VMware Tools 12.0.6 Release Notes](#)
- [Earlier versions of VMware Tools](#)
- [What Every vSphere Admin Must Know About VMware Tools](#)
- [VMware Tools for hosts provisioned with Auto Deploy](#)
- [Updating VMware Tools](#)

ESXi670-202210104-SG

Patch Category	Security
Patch Severity	Important
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	<ul style="list-style-type: none"> VMW_bootbank_xhci-xhci_1.0-3vmw.670.3.185.20491463
PRs Fixed	N/A
CVE numbers	N/A

Updates the `xhci-xhci` VIB.

ESXi-6.7.0-20221004001-standard

Profile Name	ESXi-6.7.0-20221004001-standard
Build	For build information, see Patches Contained in this Release .
Vendor	VMware, Inc.
Release Date	October 06, 2022
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	<ul style="list-style-type: none"> VMware_bootbank_esx-update_6.7.0-3.189.20497097 VMware_bootbank_vsanhealth_6.7.0-3.189.20235860 VMware_bootbank_esx-base_6.7.0-3.189.20497097 VMware_bootbank_vsan_6.7.0-3.189.20235859 VMware_bootbank_esx-xserver_6.7.0-3.189.20497097 VMW_bootbank_ntg3_4.1.8.0-4vmw.670.3.189.20497097
PRs Fixed	2945696, 2960623, 2977958, 2994957, 3001186, 3012635, 2992533
Related CVE numbers	N/A

- This patch updates the following issues:
 - When two NICs that use the `ntg3` driver of versions 4.1.3 and later are connected directly, not to a physical switch port, link flapping might occur. The issue does not occur on `ntg3` drivers of versions earlier than 4.1.3 or the `tg3` driver. This issue is not related to the occasional Energy Efficient Ethernet (EEE) link flapping on such NICs. The fix for the EEE issue is to use an `ntg3` driver of version 4.1.7 or later, or disable EEE on physical switch ports.
 - Rarely, due to the fast suspend resume mechanism used to create or revert a VM to a snapshot, the internal state of the VMX process might reinitialize without notification to the upper layers of the virtual infrastructure management stack. As a result, all guest-related performance counters that VMware Tools provides stop updating. In all interfaces to the ESXi host, you continuously see the last recorded values.
 - In rare cases, VM events might report the `template` property, which indicates if a virtual machine is marked as a template, incorrectly. As a result, you might see the `template` property as `true` even if the VM is not a template VM or as `false`, when a VM is marked as a template.
 - In an ALUA target, if the target port group IDs (TPGIDs) are changed for a LUN, the cached device identification response that SATP uses might not update accordingly. As a result, ESXi might not reflect the correct path states for the corresponding device.
 - Migrating virtual machines with RDM disks by using vSphere Storage vMotion might fail due to a mismatch of the VML IDs that identify the storage devices on the ESXi hosts in a cluster.
 - Due to a missing Memory Module Entity for Cisco servers in the Managed Object Browser, you might not see the memory status info of an ESXi host by using MOB.
 - Due to a possible timeout of I/O requests during a cross-host Storage vMotion operation, the migration task might fail and as a result, some virtual machines become unresponsive.
 - If a running virtual machine reboots during a snapshot deletion operation, the VM disks might be incorrectly reopened and closed during the snapshot consolidation. As a result, the VM might fail. However, this is a timing issue and occurs accidentally.

ESXi-6.7.0-20221004001-no-tools

Profile Name	ESXi-6.7.0-20221004001-no-tools
Build	For build information, see Patches Contained in this Release .
Vendor	VMware, Inc.
Release Date	October 06, 2022
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	<ul style="list-style-type: none"> VMware_bootbank_esx-update_6.7.0-3.189.20497097 VMware_bootbank_vsanhealth_6.7.0-3.189.20235860 VMware_bootbank_esx-base_6.7.0-3.189.20497097 VMware_bootbank_vsan_6.7.0-3.189.20235859 VMware_bootbank_esx-xserver_6.7.0-3.189.20497097 VMW_bootbank_ntg3_4.1.8.0-4vmw.670.3.189.20497097
PRs Fixed	2945696, 2960623, 2977958, 2994957, 3001186, 3012635, 2992533
Related CVE numbers	N/A

- This patch updates the following issues:
 - When two NICs that use the `ntg3` driver of versions 4.1.3 and later are connected directly, not to a physical switch port, link flapping might occur. The issue does not occur on `ntg3` drivers of versions earlier than 4.1.3 or the `tg3` driver. This issue is not related to the occasional Energy Efficient Ethernet (EEE) link flapping on such NICs. The fix for the EEE issue is to use an `ntg3` driver of version 4.1.7 or later, or disable EEE on physical switch ports.
 - Rarely, due to the fast suspend resume mechanism used to create or revert a VM to a snapshot, the internal state of the VMX process might reinitialize without notification to the upper layers of the virtual infrastructure management stack. As a result, all guest-related performance counters that VMware Tools provides stop updating. In all interfaces to the ESXi host, you continuously see the last recorded values.
 - In rare cases, VM events might report the `template` property, which indicates if a virtual machine is marked as a template, incorrectly. As a result, you might see the `template` property as `true` even if the VM is not a template VM or as `false`, when a VM is marked as a template.
 - In an ALUA target, if the target port group IDs (TPGIDs) are changed for a LUN, the cached device identification response that SATP uses might not update accordingly. As a result, ESXi might not reflect the correct path states for the corresponding device.
 - Migrating virtual machines with RDM disks by using vSphere Storage vMotion might fail due to a mismatch of the VML IDs that identify the storage devices on the ESXi hosts in a cluster.
 - Due to a missing Memory Module Entity for Cisco servers in the Managed Object Browser, you might not see the memory status info of an ESXi host by using MOB.
 - Due to a possible timeout of I/O requests during a cross-host Storage vMotion operation, the migration task might fail and as a result, some virtual machines become unresponsive.
 - If a running virtual machine reboots during a snapshot deletion operation, the VM disks might be incorrectly reopened and closed during the snapshot consolidation. As a result, the VM might fail. However, this is a timing issue and occurs accidentally.

ESXi-6.7.0-20221001001s-standard

Profile Name	ESXi-6.7.0-20221001001s-standard
Build	For build information, see Patches Contained in this Release .
Vendor	VMware, Inc.
Release Date	October 06, 2022
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	<ul style="list-style-type: none"> VMware_bootbank_esx-base_6.7.0-3.185.20491463 VMware_bootbank_esx-update_6.7.0-3.185.20491463 VMware_bootbank_vsan_6.7.0-3.185.20179805 VMware_bootbank_vsanhealth_6.7.0-3.185.20179806 VMware_bootbank_esx-ui_1.43.10-20199807 VMware_locker_tools-light_12.0.6.20104755-20491463 VMW_bootbank_xhci-xhci_1.0-3vmw.670.3.185.20491463
PRs Fixed	2994841, 2994849, 2994852, 2994853, 3001982, 3015508, 3015657
Related CVE numbers	N/A

- This patch updates the following issues:
 - ESXi670-202210001 provides the following security updates:

- cURL is updated to version 7.84.0.
- The OpenSSL library is updated to versions 1.0.2zf.
- The SQLite database is updated to version 3.39.0.
- The tcpdump package is updated to version 4.9.1.
- This release resolves CVE-2022-31681. For more information on this vulnerability and its impact on VMware products, see [VMSA-2022-0025](#).
- This release resolves CVE-2018-5733. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of [7.5](#).
- **The following VMware Tools ISO images are bundled with ESXi 670-202210001:**
 - **windows.iso:** VMware Tools 12.0.6 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
 - **linux.iso:** VMware Tools 10.3.24 ISO image for Linux OS with glibc 2.11 or later.
 - The following VMware Tools ISO images are available for download:
 - VMware Tools 11.0.6:
 - **windows.iso:** for Windows Vista (SP2) and Windows Server 2008 Service Pack 2 (SP2).
 - VMware Tools 10.0.12:
 - **winPreVista.iso:** for Windows 2000, Windows XP, and Windows 2003.
 - **linuxPreGlibc25.iso:** supports Linux guest operating systems earlier than Red Hat Enterprise Linux (RHEL) 5, SUSE Linux Enterprise Server (SLES) 11, Ubuntu 7.04, and other distributions with glibc version earlier than 2.5.
 - **solaris.iso:** VMware Tools image 10.3.10 for Solaris.
 - **darwin.iso:** Supports Mac OS X versions 10.11 and later.
 - Follow the procedures listed in the following documents to download VMware Tools for platforms not bundled with ESXi:
 - [VMware Tools 12.0.6 Release Notes](#)
 - [Earlier versions of VMware Tools](#)
 - [What Every vSphere Admin Must Know About VMware Tools](#)
 - [VMware Tools for hosts provisioned with Auto Deploy](#)
 - [Updating VMware Tools](#)

ESXi-6.7.0-20221001001s-no-tools

Profile Name	ESXi-6.7.0-20221001001s-no-tools
Build	For build information, see Patches Contained in this Release .
Vendor	VMware, Inc.
Release Date	October 06, 2022
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	<ul style="list-style-type: none"> • VMware_bootbank_esx-base_6.7.0-3.185.20491463 • VMware_bootbank_esx-update_6.7.0-3.185.20491463 • VMware_bootbank_vsan_6.7.0-3.185.20179805 • VMware_bootbank_vsanhealth_6.7.0-3.185.20179806 • VMware_bootbank_esx-ui_1.43.10-20199807 • VMware_locker_tools-light_12.0.6.20104755-20491463 • VMW_bootbank_xhci-xhci_1.0-3vmw.670.3.185.20491463
PRs Fixed	2994841, 2994849, 2994852, 2994853, 3001982, 3015508
Related CVE numbers	N/A

- This patch updates the following issues:
 - ESXi670-202210001 provides the following security updates:
 - cURL is updated to version 7.84.0.
 - The OpenSSL library is updated to versions 1.0.2zf.
 - The SQLite database is updated to version 3.39.0.
 - The tcpdump package is updated to version 4.9.1.
 - This release resolves CVE-2022-31681. For more information on this vulnerability and its impact on VMware products, see [VMSA-2022-0025](#).
 - This release resolves CVE-2018-5733. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of [7.5](#).

Known Issues

The known issues are grouped as follows.

- [Installation, Upgrade and Migration Issues](#)
- [Miscellaneous Issues](#)
- [Known Issues from Prior Releases](#)

Installation, Upgrade and Migration Issues

- **After update to ESXi670-202210001, you see an error for failed verification of the VIB signature for the esx-ui VIB**

After you complete an update to ESXi670-202210001, in the `esxupdate.log` for the `esx-ui` VIB you might see an error such as: `esxupdate: xxxxx: root: ERROR: Failed to verify VIB signature #2: ('VMware_bootbank_esx-ui_xxxxx', 'Could not find a trusted signer: self signed certificate')` The issue affects VIBs signed with keys expired on or after July 19, 2019, to align with NIAP compliance.

Workaround: Ignore the message. For more information, see VMware knowledge base article [76276](#).

Miscellaneous Issues

- **When you add or edit ESXi users by using the VMware Host Client, you see the option Enable Shell Access**

When you log in to ESXi by using the VMware Host Client to modify or create ESXi users, you see the option **Enable Shell Access** along with the required user name, description and password. However, this option works only for users with full access admin permissions.

Workaround: None.

- **ESXi hosts might fail with a purple diagnostic screen and a #PF Exception 14 for the qfle3f driver**

An issue with the `qfle3f` driver when it loses Fibre Channel over Ethernet (FCoE) connections might cause ESXi hosts to fail with a purple diagnostic screen. In the error screen, you see messages such as: `@BlueScreen: #PF Exception 14 in world 1001390820:qcnlc IP 0xXXXXX addr 0xXX`. The issue might trigger when you unload the `qfle3f` driver, reboot the ESXi host or switch or disable the FCoE port or link.

Workaround: None.

Known Issues from Prior Releases

To view a list of previous known issues, click [here](#).

Copyright © Broadcom