VMware ESXi 7.0 Update 3i Release Notes

ESXi 7.0 Update 3i | DEC 08 2022 | 20842708

Check for additions and updates to these release notes.

What's in the Release Notes

The release notes cover the following topics:

IMPORTANT: If your source system contains hosts of versions between ESXi 7.0 Update 2 and Update 3c, and Intel drivers, before upgrading to ESXi 7.0 Update 3i, see the What's New section of the VMware vCenter Server 7.0 Update 3c Release Notes, because all content in the section is also applicable for vSphere 7.0 Update 3i. Also, see the related VMware knowledge base articles: 86447, 87258, and 87308.

What's New

- ESXi 7.0 Update 3i supports vSphere Quick Boot on the following server:
    - HPE ProLiant MicroServer Gen10 Plus v2
- This release resolves CVE-2022-31696, and CVE-2022-31699. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2022-0030.

Earlier Releases of ESXi 7.0

New features, resolved, and known issues of ESXi are described in the release notes for each release. Release notes for earlier releases of ESXi 7.0 are:

- VMware ESXi 7.0, ESXi 7.0 Update 3g Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3f Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1e Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 3c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 2 Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1d Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1c Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1b Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1a Release Notes
- VMware ESXi 7.0, ESXi 7.0 Update 1 Release Notes
- VMware ESXi 7.0, ESXi 7.0b Release Notes

For internationalization, compatibility, and open source components, see the VMware vSphere 7.0 Release Notes.

Patches Contained in This Release

This release of ESXi 7.0 Update 3i delivers the following patches:

Build Details

Download Filename:	VMware-ESXi-7.0U3i-20842708-depot
Build:	20842708
Download Size:	570.5 MB
md5sum:	7ec976758701d4287393aebcc2c5d55c
sha256checksum:	26b26ddb4e0d3ba2bc4ac3b693addb111a0b1980abf03fce243473812ec460f7
Host Reboot Required:	Yes

Virtual Machine Migration or Shutdown Required:	Yes

Components

Component	Bulletin	Category	Severity
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.65.20842708	Bugfix	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.65.20842708	Bugfix	Critical
Broadcom NetXtreme I ESX VMKAPI ethernet driver	Broadcom-ntg3_4.1.8.0-4vmw.703.0.65.20842708	Bugfix	Critical
ESXi Component - core ESXi VIBs	ESXi_7.0.3-0.60.20841705	Security	Critical
ESXi Install/Upgrade Component	esx-update_7.0.3-0.60.20841705	Security	Critical
ESXi Tools Component	VMware-VM-Tools_12.1.0.20219665-20841705	Security	Critical

IMPORTANT:

- Starting with vSphere 7.0, VMware uses components for packaging VIBs along with bulletins. The `ESXi` and `esx-update` bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.
- When patching ESXi hosts by using VMware Update Manager from a version prior to ESXi 7.0 Update 2, it is strongly recommended to use the rollup bulletin in the patch baseline. If you cannot use the rollup bulletin, be sure to include *all* of the following packages in the patching baseline. If the following packages are not included in the baseline, the update operation fails:
  - VMware-vmkusb_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkata_0.1-1vmw.701.0.0.16850804 or higher
  - VMware-vmkfcoe_1.0.0.2-1vmw.701.0.0.16850804 or higher
  - VMware-NVMeoF-RDMA_1.0.1.2-1vmw.701.0.0.16850804 or higher

Rollup Bulletin

This rollup bulletin contains the latest VIBs with all the fixes after the initial release of ESXi 7.0.

Bulletin ID	Category	Severity	Detail
ESXi70U3i-20842708	Bugfix	Critical	Security and Bugfix
ESXi70U3si-20841705	Security	Critical	Security only

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-7.0U3i-20842708-standard
ESXi-7.0U3i-20842708-no-tools
ESXi-7.0U3si-20841705-standard
ESXi-7.0U3si-20841705-no-tools

ESXi Image

Name and Version	Release Date	Category	Detail
ESXi_7.0.3-0.65.20842708	DEC 08 2022	Enhancement	Security and Bugfix image
ESXi_7.0.3-0.60.20841705	DEC 08 2022	Enhancement	Security only image

For information about the individual components and bulletins, see the Product Patches page and the Resolved Issues section.

Patch Download and Installation

In vSphere 7.x, the Update Manager plug-in, used for administering vSphere Update Manager, is replaced with the Lifecycle Manager plug-in. Administrative operations for vSphere Update Manager are still available under the Lifecycle Manager plug-in, along with new capabilities for vSphere Lifecycle Manager.
The typical way to apply patches to ESXi 7.x hosts is by using the vSphere Lifecycle Manager. For details, see About vSphere Lifecycle Manager and vSphere Lifecycle Manager Baselines and Images.
You can also update ESXi hosts without using the Lifecycle Manager plug-in, and use an image profile instead. To do this, you must manually download the patch offline bundle 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 **7.0**. For more information, see the Upgrading Hosts by Using ESXCLI Commands and the VMware ESXi Upgrade guide.

Product Support Notices

- Starting with vSphere 7.0 Update 3i, when you configure the reverse proxy on the vCenter Server system to enable smart card authentication, you must use port 3128, which is set and opened automatically, but you must be permitted access to the port on the respective vCenter Server. Check your perimeter firewalls to ensure that access has been granted. Make sure you restart the STS service after you configure the rhttpproxy service.
  For more information, see Configure the Reverse Proxy to Request Client Certificates and VMware knowledge base articles 78057 and 90542.

Resolved Issues

The resolved issues are grouped as follows.

ESXi_7.0.3-0.65.20842708

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	• VMware_bootbank_esx-xserver_7.0.3-0.65.20842708 • VMware_bootbank_gc_7.0.3-0.65.20842708 • VMware_bootbank_vsan_7.0.3-0.65.20842708 • VMware_bootbank_cpu-microcode_7.0.3-0.65.20842708 • VMware_bootbank_crx_7.0.3-0.65.20842708 • VMware_bootbank_esx-base_7.0.3-0.65.20842708 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.65.20842708 • VMware_bootbank_vsanhealth_7.0.3-0.65.20842708 • VMware_bootbank_native-misc-drivers_7.0.3-0.65.20842708 • VMware_bootbank_esx-ui_2.1.1-20188605 • VMware_bootbank_trx_7.0.3-0.65.20842708 • VMware_bootbank_bmcal_7.0.3-0.65.20842708 • VMware_bootbank_vdfs_7.0.3-0.65.20842708 • VMware_bootbank_esxio-combiner_7.0.3-0.65.20842708
PRs Fixed	2962719, 3021935, 2994966, 2983919, 3014323, 2996511, 2982013, 3011324, 3048788, 2983043, 3035934, 3015498, 3031708, 3041100, 3044475, 2990414, 3003866, 3011850, 3002779, 3033161, 3016132, 3015493, 3029194, 3007116, 2977496, 3021384, 2988179, 3025470, 3033159, 3011169, 3018832, 2977486, 2932056, 3013368, 2995471, 3006356, 2981272, 3000195, 3026623, 2981420, 3025469, 3042776, 2916160, 2996208, 3014374, 2977957, 2979281, 2976953, 2999968, 3031566, 3036859, 3029490, 2992407
CVE numbers	N/A

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

Updates the `esx-xserver, gc, vsan, cpu-microcode, esx-base, esx-dvfilter-generic-fastpath, vsanhealth, native-misc-drivers, esx-ui, trx, bmcal, vdfs, esxio-combiner,` and `crx` VIBs to resolve the following issues:

- **NEW PR 2962719: Virtual machines might intermittently experience soft lockups inside the guest kernel on Intel machines**
  Starting with 7.0 Update 2, ESXi supports Posted Interrupts (PI) on Intel CPUs for PCI passthrough devices to improve the overall system performance. In some cases, a race between PIs and the VMkernel scheduling might occur. As a result, virtual machines that are configured with PCI passthrough devices with normal or low latency sensitivity might experience soft lockups.

  This issue is resolved in this release.

- **PR 3021935: 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 2994966: 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 2983919: Unresponsive Active Directory domain controllers might intermittently cause the hostd service to become unresponsive too**
  In very rare occasions, random issues with Active Directory environments that might lead to unresponsive state of the domain controllers, might also result in unresponsiveness of the hostd service.

  This issue is resolved in this release. The fix makes the hostd service resilient to intermittent Active Directory domain controller unresponsiveness.

- **PR 3014323: 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 2996511: The rhttpproxy service occasionally fails with a coredump reporting a buffer overflow**
  When the rhttpproxy service performs multiple operations on incoming URIs, it might miscalculate the buffer offset of each connection, which potentially leads to errors such as buffer overflows and negative reads. As a result, the service fails.

  This issue is resolved in this release.

- **PR 2982013: You cannot modify a hypercall option when a virtual machine is powered on**
  By default, modifying hypercall options by using commands such as `vm | Get-AdvancedSetting -Name isolation.tools.autoInstall.disable` works only when the VM is powered off. For powered on VMs such calls trigger the error `The attempted operation cannot be performed in the current state (Powered on).` This is expected.

  This issue is resolved in this release.

- **PR 3011324: Update from ESXi 7.0 Update 3c to a later version might revert to default values all security advanced options of an ESXi host**
  After you update an ESXi 7.0 Update 3c host to a later version of 7.0.x or install or remove an ESXi 7.0 Update 3c VIB and reboot the host, you might see all security advanced options on the host revert to their default values. The affected advanced settings are:
  Security.AccountLockFailures
  Security.AccountUnlockTime
  Security.PasswordQualityControl
  Security.PasswordHistory
  Security.PasswordMaxDays
  Security.SshSessionLimit
  Security.DefaultShellAccess

  This issue is resolved in this release.

- **PR 3048788: SR-IOV devices might report incorrect NUMA node for Virtual Functions**
  The command `esxcli hardware pci list`, which reports the NUMA node for ESXi host devices, returns the correct NUMA node for the Physical Functions (PF) of an SR-IOV device, but returns zero for its Virtual Functions (VF).

  This issue is resolved in this release. The fix makes sure that NUMA nodes are consistent for both PF and VF of SR-IOV devices.

- **PR 2983043: Windows Guest OS might fail with a blue diagnostic screen after migration of virtual machines to ESXi hosts of version 7.0 Update 2 or later**
  After an upgrade to ESXi 7.0 Update 2 or later, when you migrate Windows virtual machines to the upgraded hosts by using vSphere vMotion, some VMs might fail with a blue diagnostic screen after the migration. In the screen, you see the error `OS failed to boot with no operating system found`. The issue occurs due to a fault in the address optimization logic of the Virtual Machine File System (VMFS).

  This issue is resolved in this release.

- **PR 3035934: ESXi hosts might become unresponsive when no registered default request handler is available and the execution of vmacore.dll fails**
  If the client application has no registered default request handler, requests with a path that is not present in the handler map might cause the execution of `vmacore.dll` to fail. As a result, you see the ESXi host as disconnected from the vCenter Server system.

  This issue is resolved in this release.

- **PR 3015498: ESXi hosts might fail with a purple diagnostic screen during resource allocation reservation operations**
  Some allocation reservation operations might go over the limit of 128 parallel reservation keys and exceed the allocated memory range of an ESXi host. As a result, ESXi hosts might fail with a purple diagnostic screen during resource allocation reservation operations. In the error screen, you see messages such as `PSOD BlueScreen: #PF Exception 14 in world 2097700:SCSI period IP`.

  This issue is resolved in this release.

- **PR 3031708: ESXi hosts might fail with a purple diagnostic screen during device or path unclaim operations**

If you run an unclaim command on a device or path while virtual machines on the device still have active I/Os, the ESXi host might fail with a purple diagnostic screen. In the screen, you see a message such as `PSOD at bora/modules/vmkernel/nmp/nmp_misc.c:3839 during load/unload of lpfc.`

This issue is resolved in this release.

- **PR 3041100: When TPM 2.0 is enabled with TXT on an ESXi host, attempts to power-on a virtual machine might fail**
  When TXT is enabled on an ESX host, attempts to power-on a VM might fail with an error. In the vSphere Client, you see a message such as `This host supports Intel VT-x, but Intel VT-x is restricted. Intel VT-x might be restricted because 'trusted execution' has been enabled in the BIOS/firmware settings or because the host has not been power-cycled since changing this setting.`

  This issue is resolved in this release.

- **PR 3044475: Virtual machines might fail with ESX unrecoverable error due to a rare issue with handling AVX2 instructions**
  Due to a rare issue with handling AVX2 instructions, a virtual machine of version ESX 7.0 Update 3f might fail with ESX unrecoverable error. In the `vmware.log` file, you see a message such as: `MONITOR PANIC: vcpu-0:VMM fault 6: src=MONITOR ....`
  The issue is specific for virtual machines with hardware versions 12 or earlier.

  This issue is resolved in this release.

- **PR 2990414: Upgrade operations by using a vSphere Lifecycle Manager upgrade baseline with a vSphere ESXi Image Builder .iso custom image might fail**
  If you use an ESXi `.iso` image created by using the Image Builder to make a vSphere Lifecycle Manager upgrade baseline for ESXi hosts, upgrades by using such baselines might fail. In the vSphere Client, you see an error such as `Cannot execute upgrade script on host`. On the impacted ESXi host, in the `/var/log/vua*.log` file, you see an error such as `ValueError: Should have base image when an addon exists`.
  The error occurs when the existing image of the ESXi host has an add-on, but the Image Builder-generated ISO provides no add-on.

  This issue is resolved in this release.

- **PR 3003866: ESXi hosts might fail with a purple diagnostic screen due to insufficient XMAP space**
  Many parallel requests for memory regions by virtual machines using the Data Plane Development Kit (DPDK) on an ESXi host might exceed the XMAP memory space on the host. As a result, the host fails with a purple diagnostic screen and an error such as: `Panic Message: @BlueScreen: VERIFY bora/vmkernel/hardware/pci/config.c:157.`

  This issue is resolved in this release. The fix sets the default memory regions available for all vmxnet3 adapters to 8192 MB.

- **PR 3011850: You do not see some performance reports for virtual machines with NVMe controllers on ESXi 7.0 Update 3 and later**
  After an upgrade of ESXi hosts to ESXi 7.0 Update 3 and later, you might no longer see some performance reports for virtual machines with NVMe controllers. For example, you do not see the Virtual Disk - Aggregate of all Instances chart in the VMware Aria Operations.

  This issue is resolved in this release.

- **PR 3002779: ESXi host with a Fault Tolerance encryption enabled secondary VM might fail with a purple diagnostic screen due to a decryption buffer overflow**
  In rare cases, such as scheduled reboot of the primary VM with FT encryption that runs heavy workloads, the secondary VM might not have sufficient buffer to decrypt more than 512 MB of dirty pages in a single FT checkpoint and experience a buffer overflow error. As a result, the ESXi host on which the secondary VM resides might fail with a purple diagnostic screen.

  This issue is resolved in this release.

- **PR 3033161: After upgrade or update to ESXi 7.0 Update 2 and later, vSAN storage marked as flash (SSD) might change to magnetic disk (HDD)**
  In rare cases, after upgrade or update to ESXi 7.0 Update 2 and later, the vSAN storage configuration might lose the tag `mark_ssd` and default to HDD.

  This issue is resolved in this release.

- **PR 3016132: You see frequent logs for failed registration of detached LUNs**
  Even when a device or LUN is in a detached state, the Pluggable Storage Architecture (PSA) might still attempt to register the object. PSA files a log for each path evaluation step at every path evaluation interval of such attempts. As a result, you might see multiple identical messages such as `nmp_RegisterDeviceEvents failed` for device registration, which are not necessary while the device or LUN is detached.

  This issue is resolved in this release.

- **PR 3015493: When you change a device configuration at runtime, a datastore might fail to mount after an ESXi host reboots**
  If you change a device configuration at runtime, changes might not be reflected in the ESXi ConfigStore that holds the configurations for an ESXi host. As a result, the datastore might not mount after the ESXi host reboots.

  This issue is resolved in this release. The fix makes sure that ConfigStore reflects device configuration changes at runtime.

- **PR 3029194: After upgrade to ESXi 7.0 Update 3 and later, ESXi hosts might fail with a purple diagnostic screen due to legacy I/O scheduler**
  Starting from ESXi 6.0, mClock is the default I/O scheduler for ESXi, but some environments might still use legacy schedulers of ESXi versions earlier than 6.0. As a result, upgrades of such hosts to ESXi 7.0 Update 3 and later might fail with a purple diagnostic screen.

  This issue is resolved in this release.

- **PR 3007116: If you upgrade ESXi hosts to ESXi 7.0 Update 3d or later by using a host profile with tokens indicating ALUA state, the host might fail with a purple diagnostic screen**
  Starting with ESXi 7.0 Update 1, the configuration management of ESXi hosts moved from the `/etc/vmware/esx.conf` file to the ConfigStore framework, which makes an explicit segregation of state and configuration. Tokens in the `esx.conf` file such as `implicit_support` or `explicit_support` that indicate a state, are not recognized as valid tokens, and are ignored by the `satp_alua` module. As a result, when you upgrade ESXi hosts to ESXi 7.0 Update 3d or later by using a host profile with tokens indicating ALUA state, the operation might fail with a purple diagnostic screen. In the screen, you see an error such as `Failed modules: /var/lib/vmware/configmanager/upgrade/lib/postLoadStore/libupgradepsadeviceconfig.so`.

  This issue is resolved in this release.

- **PR 2977496: An ESXi host might become unresponsive due to a rare file block (FB) allocation issue**
  A helper mechanism that caches FB resource allocation details working in background might accidentally stop and block FB resource allocation during I/O operations to the ESXi host. In some cases, this issue might affect other processes working on the same file and block them. As a result, the ESXi host might become unresponsive.

  This issue is resolved in this release.

- **PR 3021384: vSAN File Service fails to enable when an isolated witness network is configured**
  vSAN File Service requires hosts to communicate with each other. File Service might incorrectly use an IP address in the witness network for inter-communication. If you have configured an isolated witness network for vSAN, the host can communicate with a witness node over the witness network, but hosts cannot communicate with each other over the witness network. Communication between hosts for vSAN File Service cannot be established.

  This issue is resolved in this release.

- **PR 2988179: If an ESXi host is in a low memory state, insufficient heap allocation to a network module might cause the host to fail with a purple diagnostic screen**
  If an ESXi host is in a low memory state, insufficient heap allocation to a network module might cause the port bitmap to be set to `NULL`. As a result, the ESXi host might fail with a purple diagnostic screen when attempting to forward a packet.

  This issue is resolved in this release. The fix makes sure that bit vectors in the `portsBitmap` property are set only when heap allocation is successful. However, you still need to make sure that ESXi hosts have sufficient RAM to operate and forward packets successfully.

- **PR 3025470: The Cluster Level Object Manager Daemon (CLOMD) fails during object format change**
  During object format change, some objects with old layout might get partially cleaned up, leaving the configuration in an invalid state. This problem can cause CLOMD to fail whenever it attempts to process the object during reconfiguration.

  You might see the following entries in `clomd.log` file:

  ```
  2022-10-14T16:17:26.456Z PANIC: NOT_REACHED bora/lib/vsan/vsan_config_builder.c:744
  2022-10-14T16:17:26.456Z Backtrace:
  2022-10-14T16:17:26.456Z Backtrace[0] 0000030b4742c6a0 rip=000000bf0c7de98f rbx=0000030b4742c6a0
  rbp=0000030b4742cad0 r12=000000bf0d677788 r13=0000030b4742cae8 r14=000000bf14ce052c r15=000000bf14ce3c2c
  ```

  This issue is resolved in this release.

- **PR 3033159: ESXi hosts might fail with a purple diagnostic screen when a VM with bus sharing set to Physical issues a SCSI-2 reserve command**
  Windows 2012 and later use SCSI-3 reservation for resource arbitration to support Windows failover clustering (WSFC) on ESXi for cluster-across-box (CAB) configurations. However, if you configure the bus sharing of the SCSI controller on that VM to `Physical`, the `SCSI RESERVE` command causes the ESXi host to fail with a purple diagnostic screen. `SCSI RESERVE` is SCSI-2 semantic and is not supported with WSFC clusters on ESXi.

  This issue is resolved in this release.

- **PR 3011169: vSAN cluster congestion due to cache buildup**
  vSAN might stop destaging data due to a counting issue of outstanding I/Os. If a VSAN disk group stops destaging data from the cache to the capacity tier, this can cause data to accumulate in the cache tier. This problem leads to congestion, I/O throttling, and longer latency.

  This issue is resolved in this release.

- **PR 3018832: If a cluster contains a 0-byte object, vSAN hosts might fail with a purple diagnostic screen**
  If a vSAN cluster with a 0-byte object receives a policy change request, the Cluster Level Object Manager (CLOM) might incorrectly set an invalid flag for one or more components of the object. Such a flag can cause the host to send large writes that overload the system and cause the host to fail with a purple diagnostic screen.

  This issue is resolved in this release.

- **PR 2977486: Intermittent lock contention for VMFS journal blocks might delay VMFS rescan commands or cause mounting a datastore to fail**
  A rare issue with processing VMFS journal blocks might cause lock contention that results in delays of VMFS rescan operations or failed mounting of datastores. In the vmkernel logs, you see errors such as `Resource file for resource: 6 reached max limit 8192` and `Resource file extension ('No space left on device')`.

  This issue is resolved in this release.

- **PR 2932056: The vmx service might fail during cancellation of a vSphere Storage vMotion task and vCenter Server High Availability restarts virtual machines**
  In rare cases, the vmx service might fail during the cancellation of a vSphere Storage vMotion task. As a result, if your environment uses vCenter Server High Availability, the service restarts the affected virtual machines.

  This issue is resolved in this release.

- **PR 3013368: During booting, you see errors that support for SD Card and USB-only configurations is deprecated**
  When you use setups with only SD or USB devices to boot ESXi 7.x, you might see errors such as `support for SD-Card/USB only configuration is being deprecated`. This message does not indicate an error, but only a warning that SD and USB devices are supported only for bootbank partitions, and for best performance, a secondary persistent storage with a minimum of 32 GB must be provided for the `/scratch` and VMware Tools which reside in the OSData partition.

  This issue is resolved in this release. The fix removes the message to avoid confusion, as deployments with no persistent storage are supported, although not a best practice.

- **PR 2995471: vSAN disk encrypted and locked due to encryption key not available**
  This issue applies to vSAN hosts that use an external KMS for data-at-rest encryption. When you upgrade a vSAN host from 6.7 or earlier to 7.0 and later, the KMS password is lost. The host's disks remain encrypted and locked.

  This issue is resolved in this release.

- **PR 3006356: ESXi host fail with a purple diagnostic screen due to rebinding of virtual volumes**
  In rare cases, vSphere Virtual Volumes might attempt to rebind volumes on ESXi hosts that have SCSI Persistent Reservations. As a result, the ESXi hosts fail with a purple diagnostic screen and an error such as `Panic Message: @BlueScreen: PANIC bora/vmkernel/main/dlmalloc.c:4933 - Usage error in dlmalloc` in the backtrace.

  This issue is resolved in this release.

- **PR 2981272: vSphere Client displays 0 KB regardless of the actual VMDK size of a virtual machine**
  Due to a caching issue, in the vSphere Client you might see a VMDK size of 0 KB regardless of the actual size of virtual machines in a vSphere Virtual Volumes environment.

  This issue is resolved in this release.

- **PR 3000195: A cross site Advanced Cross vCenter vMotion operation might timeout and some virtual machines become unresponsive**
  During the storage migration part of a cross site Advanced Cross vCenter vMotion operation, some async I/Os at the storage stack might be trapped and not properly time out. As a result, virtual machines remain waiting for a I/O response, which causes the Advanced Cross vCenter vMotion operation to time out and the virtual machines to become unresponsive.

  This issue is resolved in this release. The fix adds a timeout to every async I/O request to makes sure that a response is returned after the timeout.

- **PR 3026623: LLOG recovery might erroneously mark vSAN components as invalid**
  A problem during LLOG recovery can cause a vSAN component to be erroneously marked as invalid. This issue can lead to log build up and congestion.

  This issue is resolved in this release.

- **PR 2981420: The Small-Footprint CIM Broker Daemon (SFCBD) intermittently fails**
  Due to insufficient resource pool allocation, some services that report to the SFCBD, such as sfcb-vmware_base and sfcb-vmw, might fail and generate zdump. In the `syslog.log` file you see errors such as:
  ```
  sfcb-vmware_base[2110110]: tool_mm_realloc_or_die: memory re-allocation failed(orig=364000 new=364800 msg=Cannot allocate memory, aborting
  sfcb-vmw_ipmi[2291550]: tool_mm_realloc_or_die: memory re-allocation failed(orig=909200 new=909600 msg=Cannot allocate memory, aborting
  ```

  This issue is resolved in this release. The fix increases the default pool size for sfcb-vmware_base service.

- **PR 3025469: If the target policy is Raid 1, StripeWidth 1, policy reconfiguration of large objects in a vSAN cluster might stop with no progress**
  If the target policy is Raid 1, StripeWidth 1, when a vSAN cluster runs low on transient capacity, the Cluster Level Object Manager might keep reconfiguring the same part of objects larger than 8TB. As a result, such objects remain in noncompliant state, and you might see some unnecessary resync operations.

  This issue is resolved in this release.

- **PR 3042776: Storage I/O Control quickly generates a large volume of logs marked as critical that might also fill up the datastore**
  In VMware Aria Operations for Logs, formerly vRealize Log Insight, you might see a large volume of logs generated by Storage I/O Control such as `Invalid share value: 0. Using default.` and `Skipping device naa.xxxx either due to VSI read error or abnormal state`. The volume of logs varies depending on the number of ESXi hosts in a cluster and the number of devices in switched off state. When the issue occurs, the log volume generates quickly, within 24 hours, and VMware Aria Operations for Logs might classify the messages as critical. However, such logs are harmless and do not impact the operations on other datastores that are online.

  This issue is resolved in this release. The fix moves such logs from error to trivia to prevent misleading logging.

- **PR 2916160: ESXi Managed Object Browser (MOB) shows the CPU status as unknown**
  If the storage sensor list of an ESXi host is empty, the CPU status that the Intelligent Platform Management Interface (IPMI) reports might reset. As a result, you see the sensor data record with `entity ID 3`, which is the status of the processor, displayed incorrectly as `Cannot report on the current status of the physical element` in the MOB.

This issue is resolved in this release. The fix makes sure that the CPU status resets only when refreshing the sensor state from IPMI fails.

- **PR 2996208: You see high read latency for objects in a stretch cluster**
  In stretch clusters, vSAN deploys each VMDK object with a specific format. When you change the policy of a VMDK object from `hostFailuresToTolerate=0` to `hostFailuresToTolerate=1`, the format might change in such a way that it can cause reads to transit the inter-site(cross-AZ) link. As a result, you see higher read latency in such objects.

  This issue is resolved in this release.

- **PR 3014374: In the vSphere Client, you see repeated options in the SCSI Bus Sharing drop-down menu**
  In the vSphere Client, when you create or reconfigure a virtual machine, under **SCSI controller** > **SCSI Bus Sharing** you might see doubling options in the drop-down menu. The issue does not affect any of the VM create or configure workflows.

  This issue is resolved in this release.

- **PR 2977957: After a migration operation, Windows 10 virtual machines might fail with a blue diagnostic screen and reports for a microcode revision mismatch**
  After a migration operation, Windows 10 virtual machines might fail with a blue diagnostic screen and report a microcode revision mismatch error such as:- `MICROCODE_REVISION_MISMATCH (17e).` The issue occurs when a scan of the CPUs runs during the migration operation and the firmware of the source CPUs does not match with the firmware of the destination CPUs.

  This issue is resolved in this release.

- **PR 2979281: ESXi hosts might become unresponsive due to intermittent out of memory state in result of stale cache**
  In certain cases, clearing the cache of objects in a datastore volume on ESXi hosts fails, objects remain in the cache, and cause out of memory state. For example, when connection with the underlying device of the volume drops. As a result, the ESXi host becomes unresponsive. In the logs, you see errors such as: `Cannot reconnect to xxxxx] or Failed to cleanup VMFS heartbeat on volume xxxxx: No connection.` or `The volume on the device xxxxx locked, possibly because some remote host encountered an error during a volume operation and could not recover`.

  This issue is resolved in this release.

- **PR 2976953: The hostd service might fail and virtual machines shut down due to intermittent object cache exhaustion**
  Certain workflows like backup operations of ESXi hosts can open a large number of files which in turn could lead to object cache exhaustion. In such cases, you might see the hostd service to fail, or virtual machines to shut down, or the VM to get into an invalid state that prevents it to power-on. In the logs, you see warnings such as `Cannot allocate memory`.

  This issue is resolved in this release. The fix doubles the object cache size to 183 MB to fit heavy workloads.

- **PR 2999968: vSAN health reports an error that the file server is restarting**
  In **Monitor** > **Skyline Health** > **File Service** > **File Server Health**, you might see the error `File server is (re)starting`.
  The issue is caused by a cache overrun, which leads to failure of the VDFS daemon. In the `/var/run/log/vdfsd-server.log` file in an affected ESXi host, you see messages such as `NOT_IMPLEMENTED bora/vdfs/core/VDFSPhysicalLog.cpp`.

  This issue is resolved in this release.

- **PR 3031566: Changing the policy of a powered-on VM with an IDE controller throws an error that the attempted operation cannot be performed in the current state**
  In the vSphere Client, when you change the policy of a powered-on VM with an IDE controller, you might see the error `The attempted operation cannot be performed in the current state ("Powered on")`.

  This issue is resolved in this release.

- **PR 3036859: HCI Mesh fails to mount cluster after reenabling vSAN with data-in-transit encryption previously enabled**
  HCI Mesh cluster mount might fail after you deactivate vSAN with data-in-transit encryption, and then reenable vSAN.

  This issue is resolved in this release.

- **PR 3029490: vSAN Skyline Health does not include Hardware Compatibility group**
  If NVMe drives used for vSAN have a duplicate PCI ID, and you restart the vSAN health service on vCenter Server, the Hardware Compatibility group is missing from vSAN Skyline Health.

  This issue is resolved in this release.

- **PR 2992407: TPM 2.0 attestation might fail on Lenovo servers with an insufficient buffer error**
  TPM 2.0 attestation on Lenovo servers returns the TPM error code: `TSS2_SYS_RC_INSUFFICIENT_BUFFER`.

  This issue is resolved in this release.

esx-update_7.0.3-0.65.20842708

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes

Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	• VMware_bootbank_esx-update_7.0.3-0.65.20842708 • VMware_bootbank_loadesx_7.0.3-0.65.20842708
PRs Fixed	N/A
CVE numbers	N/A

Updates the `loadesx` and `esx-update` VIBs.

Broadcom-ntg3_4.1.8.0-4vmw.703.0.65.20842708

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	• VMW_bootbank_ntg3_4.1.8.0-4vmw.703.0.65.20842708
PRs Fixed	3007883
CVE numbers	N/A

Updates the `ngt3` VIB to resolve the following issue:

- **PR 3007883: 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. ESXi 7.0 Update 3i 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.

ESXi_7.0.3-0.60.20841705

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	• VMware_bootbank_esx-base_7.0.3-0.60.20841705 • VMware_bootbank_trx_7.0.3-0.60.20841705 • VMware_bootbank_vsanhealth_7.0.3-0.60.20841705 • VMware_bootbank_cpu-microcode_7.0.3-0.60.20841705 • VMware_bootbank_crx_7.0.3-0.60.20841705 • VMware_bootbank_vsan_7.0.3-0.60.20841705 • VMware_bootbank_native-misc-drivers_7.0.3-0.60.20841705 • VMware_bootbank_esx-xserver_7.0.3-0.60.20841705 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.60.20841705 • VMware_bootbank_gc_7.0.3-0.60.20841705 • VMware_bootbank_esx-ui_2.1.1-20188605 • VMware_bootbank_vdfs_7.0.3-0.60.20841705 • VMware_bootbank_bmcal_7.0.3-0.60.20841705 • VMware_bootbank_esxio-combiner_7.0.3-0.60.20841705
PRs Fixed	2993721, 3007957, 3007958, 3015560, 3034286, 3038621, 3030691
CVE numbers	CVE-2020-28196, CVE-2022-31696, CVE-2022-31699

The ESXi and esx-update bulletins are dependent on each other. Always include both in a single ESXi host patch baseline or include the rollup bulletin in the baseline to avoid failure during host patching.

Updates the `esx-ui, esx-xserver, cpu-microcode, trx, vsanhealth, esx-base, esx-dvfilter-generic-fastpath, gc, esxio-combiner, native-misc-drivers, bmcal, vsan, vdfs,` and `crx` VIBs to resolve the following issues:

- **The cpu-microcode VIB includes the following Intel microcode:**

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Nehalem EP	0x106a5 (06/1a/5)	0x03	0x0000001d	5/11/2018	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Clarkdale	0x20652 (06/25/2)	0x12	0x00000011	5/8/2018	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series
Arrandale	0x20655 (06/25/5)	0x92	0x00000007	4/23/2018	Intel Core i7-620LE Processor
Sandy Bridge DT	0x206a7 (06/2a/7)	0x12	0x0000002f	2/17/2019	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2 (06/2c/2)	0x03	0x0000001f	5/8/2018	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d6 (06/2d/6)	0x6d	0x00000621	3/4/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Sandy Bridge EP	0x206d7 (06/2d/7)	0x6d	0x0000071a	3/24/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6 (06/2e/6)	0x04	0x0000000d	5/15/2018	Intel Xeon 65xx Series; Intel Xeon 75xx Series
Westmere EX	0x206f2 (06/2f/2)	0x05	0x0000003b	5/16/2018	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9 (06/3a/9)	0x12	0x00000021	2/13/2019	Intel i3-3200 Series; Intel i7-3500-LE/UE; Intel i7-3600-QE; Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C
Haswell DT	0x306c3 (06/3c/3)	0x32	0x00000028	11/12/2019	Intel Xeon E3-1200-v3 Series; Intel i7-4700-EQ Series; Intel i5-4500-TE Series; Intel i3-4300 Series
Ivy Bridge EP	0x306e4 (06/3e/4)	0xed	0x0000042e	3/14/2019	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-1600-v2 Series; Intel Xeon E5-1400-v2 Series
Ivy Bridge EX	0x306e7 (06/3e/7)	0xed	0x00000715	3/14/2019	Intel Xeon E7-8800/4800/2800-v2 Series
Haswell EP	0x306f2 (06/3f/2)	0x6f	0x00000049	8/11/2021	Intel Xeon E5-4600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-1400-v3 Series
Haswell EX	0x306f4 (06/3f/4)	0x80	0x0000001a	5/24/2021	Intel Xeon E7-8800/4800-v3 Series
Broadwell H	0x40671 (06/47/1)	0x22	0x00000022	11/12/2019	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8 (06/4d/8)	0x01	0x0000012d	9/16/2019	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series
Broadwell EP/EX	0x406f1 (06/4f/1)	0xef	0x0b000040	5/19/2021	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Skylake SP	0x50654 (06/55/4)	0xb7	0x02006e05	3/8/2022	Intel Xeon Platinum 8100 Series; Intel Xeon Gold 6100/5100, Silver 4100, Bronze 3100 Series; Intel Xeon D-2100 Series; Intel Xeon D-1600 Series; Intel Xeon W-3100 Series; Intel Xeon W-2100 Series
Cascade Lake B-0	0x50656 (06/55/6)	0xbf	0x04003302	12/10/2021	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/Bronze 3200; Intel Xeon W-3200
Cascade Lake	0x50657 (06/55/7)	0xbf	0x05003302	12/10/2021	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/Bronze 3200; Intel Xeon W-3200
Cooper Lake	0x5065b (06/55/b)	0xbf	0x07002501	11/19/2021	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300
Broadwell DE	0x50662 (06/56/2)	0x10	0x0000001c	6/17/2019	Intel Xeon D-1500 Series
Broadwell DE	0x50663 (06/56/3)	0x10	0x0700001c	6/12/2021	Intel Xeon D-1500 Series
Broadwell DE	0x50664 (06/56/4)	0x10	0x0f00001a	6/12/2021	Intel Xeon D-1500 Series
Broadwell NS	0x50665 (06/56/5)	0x10	0x0e000014	9/18/2021	Intel Xeon D-1600 Series
Skylake H/S	0x506e3 (06/5e/3)	0x36	0x000000f0	11/12/2021	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Denverton	0x506f1 (06/5f/1)	0x01	0x00000038	12/2/2021	Intel Atom C3000 Series
Ice Lake SP	0x606a6 (06/6a/6)	0x87	0x0d000375	4/7/2022	Intel Xeon Silver 4300 Series; Intel Xeon Gold 6300/5300 Series; Intel Xeon Platinum 8300 Series
Ice Lake D	0x606c1 (06/6c/1)	0x10	0x010001f0	6/24/2022	Intel Xeon D Series
Snow Ridge	0x80665 (06/86/5)	0x01	0x4c000020	5/10/2022	Intel Atom P5000 Series
Snow Ridge	0x80667 (06/86/7)	0x01	0x4c000020	5/10/2022	Intel Atom P5000 Series
Kaby Lake H/S/X	0x906e9 (06/9e/9)	0x2a	0x000000f0	11/12/2021	Intel Xeon E3-1200-v6 Series; Intel Xeon E3-1500-v6 Series
Coffee Lake	0x906ea (06/9e/a)	0x22	0x000000f0	11/15/2021	Intel Xeon E-2100 Series; Intel Xeon E-2200 Series (4 or 6 core)
Coffee Lake	0x906eb (06/9e/b)	0x02	0x000000f0	11/12/2021	Intel Xeon E-2100 Series
Coffee Lake	0x906ec (06/9e/c)	0x22	0x000000f0	11/15/2021	Intel Xeon E-2100 Series
Coffee Lake Refresh	0x906ed (06/9e/d)	0x22	0x000000f4	7/31/2022	Intel Xeon E-2200 Series (8 core)
Rocket Lake S	0xa0671 (06/a7/1)	0x02	0x00000056	8/2/2022	Intel Xeon E-2300 Series

- **ESXi 7.0 Update 3i provides the following security updates:**
  - OpenSSL is updated to version 1.0.2zf.
  - Apache Thrift is updated to version 0.15.0.
  - The urllib3 client is updated to version 1.26.5.
  - cURL is updated to version 7.84.0.
  - The SQLite database is updated to version 3.39.2.
  - The Expat XML parser is updated to version 2.4.9.
- This release resolves CVE-2022-31696, and CVE-2022-31699. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2022-0030.

esx-update_7.0.3-0.60.20841705

Patch Category	Bugfix
Patch Severity	Critical
Host Reboot Required	Yes
Virtual Machine Migration or Shutdown Required	Yes
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	• VMware_bootbank_loadesx_7.0.3-0.60.20841705 • VMware_bootbank_esx-update_7.0.3-0.60.20841705
PRs Fixed	N/A
CVE numbers	N/A

Updates the `loadesx` and `esx-update` VIBs.

VMware-VM-Tools_12.1.0.20219665-20841705

Patch Category	Security
Patch Severity	Critical
Host Reboot Required	No
Virtual Machine Migration or Shutdown Required	No
Affected Hardware	N/A
Affected Software	N/A
VIBs Included	• VMware_locker_tools-light_12.1.0.20219665-20841705
PRs Fixed	3015499
CVE numbers	N/A

Updates the `tools-light` VIB.

- **The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3i:**
  - `windows.iso`: VMware Tools 12.1.0 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
  - `linux.iso`: VMware Tools 10.3.25 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 12.1.0 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-7.0U3i-20842708-standard

Profile Name	ESXi-7.0U3i-20842708-standard
Build	For build information, see Patches Contained in this Release.
Vendor	VMware, Inc.
Release Date	December 8, 2022
Acceptance Level	PartnerSupported
Affected Hardware	N/A

Affected Software	N/A
Affected VIBs	• VMware_bootbank_esx-xserver_7.0.3-0.65.20842708 • VMware_bootbank_gc_7.0.3-0.65.20842708 • VMware_bootbank_vsan_7.0.3-0.65.20842708 • VMware_bootbank_cpu-microcode_7.0.3-0.65.20842708 • VMware_bootbank_crx_7.0.3-0.65.20842708 • VMware_bootbank_esx-base_7.0.3-0.65.20842708 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.65.20842708 • VMware_bootbank_vsanhealth_7.0.3-0.65.20842708 • VMware_bootbank_native-misc-drivers_7.0.3-0.65.20842708 • VMware_bootbank_esx-ui_2.1.1-20188605 • VMware_bootbank_trx_7.0.3-0.65.20842708 • VMware_bootbank_bmcal_7.0.3-0.65.20842708 • VMware_bootbank_vdfs_7.0.3-0.65.20842708 • VMware_bootbank_esxio-combiner_7.0.3-0.65.20842708 • VMware_bootbank_esx-update_7.0.3-0.65.20842708 • VMware_bootbank_loadesx_7.0.3-0.65.20842708 • VMW_bootbank_ntg3_4.1.8.0-4vmw.703.0.65.20842708 • VMware_locker_tools-light_12.1.0.20219665-20841705
PRs Fixed	2962719, 3021935, 2994966, 2983919, 3014323, 2996511, 2982013, 3011324, 3048788, 2983043, 3035934, 3015498, 3031708, 3041100, 3044475, 2990414, 3003866, 3011850, 3002779, 3033161, 3016132, 3015493, 3029194, 3007116, 2977496, 3021384, 2988179, 3025470, 3033159, 3011169, 3018832, 2977486, 2932056, 3013368, 2995471, 3006356, 2981272, 3000195, 3026623, 2981420, 3025469, 3042776, 2916160, 2996208, 3014374, 2977957, 2979281, 2976953, 2999968, 3031566, 3036859, 3029490, 3007883, 2992407
Related CVE numbers	N/A

- **This patch updates the following issues:**
  - Starting with 7.0 Update 2, ESXi supports Posted Interrupts (PI) on Intel CPUs for PCI passthrough devices to improve the overall system performance. In some cases, a race between PIs and the VMkernel scheduling might occur. As a result, virtual machines that are configured with PCI passthrough devices with normal or low latency sensitivity might experience soft lockups.
  - 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.
  - 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.
  - In very rare occasions, random issues with Active Directory environments that might lead to unresponsive state of the domain controllers, might also result in unresponsiveness of the hostd service.
  - 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.
  - When the rhttpproxy service performs multiple operations on incoming URIs, it might miscalculate the buffer offset of each connection, which potentially leads to errors such as buffer overflows and negative reads. As a result, the service fails.
  - By default, modifying hypercall options by using commands such as `vm | Get-AdvancedSetting -Name isolation.tools.autoInstall.disable` works only when the VM is powered off. For powered on VMs such calls trigger the error `The attempted operation cannot be performed in the current state (Powered on).` This is expected.
  - After you update an ESXi 7.0 Update 3c host to a later version of 7.0.x or install or remove an ESXi 7.0 Update 3c VIB and reboot the host, you might see all security advanced options on the host revert to their default values. The affected advanced settings are:
    Security.AccountLockFailures
    Security.AccountUnlockTime
    Security.PasswordQualityControl
    Security.PasswordHistory
    Security.PasswordMaxDays
    Security.SshSessionLimit
    Security.DefaultShellAccess
  - The command `esxcli hardware pci list`, which reports the NUMA node for ESXi host devices, returns the correct NUMA node for the Physical Functions (PF) of an SR-IOV device, but returns zero for its Virtual Functions (VF).
  - After an upgrade to ESXi 7.0 Update 2 or later, when you migrate Windows virtual machines to the upgraded hosts by using vSphere vMotion, some VMs might fail with a blue diagnostic screen after the migration. In the screen, you see the error `OS failed to boot with no operating system found`. The issue occurs due to a fault in the address optimization logic of the Virtual Machine File System (VMFS).

- If the client application has no registered default request handler, requests with a path that is not present in the handler map might cause the execution of `vmacore.dll` to fail. As a result, you see the ESXi host as disconnected from the vCenter Server system.
- Some allocation reservation operations might go over the limit of 128 parallel reservation keys and exceed the allocated memory range of an ESXi host. As a result, ESXi hosts might fail with a purple diagnostic screen during resource allocation reservation operations. In the error screen, you see messages such as `PSOD BlueScreen: #PF Exception 14 in world 2097700:SCSI period IP`.
- If you run an unclaim command on a device or path while virtual machines on the device still have active I/Os, the ESXi host might fail with a purple diagnostic screen. In the screen, you see a message such as `PSOD at bora/modules/vmkernel/nmp/nmp_misc.c:3839 during load/unload of lpfc.`
- When TXT is enabled on an ESX host, attempts to power-on a VM might fail with an error. In the vSphere Client, you see a message such as `This host supports Intel VT-x, but Intel VT-x is restricted. Intel VT-x might be restricted because 'trusted execution' has been enabled in the BIOS/firmware settings or because the host has not been power-cycled since changing this setting`.
- Due to a rare issue with handling AVX2 instructions, a virtual machine of version ESX 7.0 Update 3f might fail with ESX unrecoverable error. In the `vmware.log` file, you see a message such as: `MONITOR PANIC: vcpu-0:VMM fault 6: src=MONITOR ....`
  The issue is specific for virtual machines with hardware versions 12 or earlier.
- If you use an ESXi `.iso` image created by using the Image Builder to make a vSphere Lifecycle Manager upgrade baseline for ESXi hosts, upgrades by using such baselines might fail. In the vSphere Client, you see an error such as `Cannot execute upgrade script on host`. On the impacted ESXi host, in the `/var/log/vua*.log` file, you see an error such as `ValueError: Should have base image when an addon exists`.
  The error occurs when the existing image of the ESXi host has an add-on, but the Image Builder-generated ISO provides no add-on.
- Many parallel requests for memory regions by virtual machines using the Data Plane Development Kit (DPDK) on an ESXi host might exceed the XMAP memory space on the host. As a result, the host fails with a purple diagnostic screen and an error such as: `Panic Message: @BlueScreen: VERIFY bora/vmkernel/hardware/pci/config.c:157.`
- After an upgrade of ESXi hosts to ESXi 7.0 Update 3 and later, you might no longer see some performance reports for virtual machines with NVMe controllers. For example, you do not see the Virtual Disk - Aggregate of all Instances chart in the VMware Aria Operations.
- In rare cases, such as scheduled reboot of the primary VM with FT encryption that runs heavy workloads, the secondary VM might not have sufficient buffer to decrypt more than 512 MB of dirty pages in a single FT checkpoint and experience a buffer overflow error. As a result, the ESXi host on which the secondary VM resides might fail with a purple diagnostic screen.
- In rare cases, after upgrade or update to ESXi 7.0 Update 2 and later, the vSAN storage configuration might lose the tag `mark_ssd` and default to HDD.
- Even when a device or LUN is in a detached state, the Pluggable Storage Architecture (PSA) might still attempt to register the object. PSA files a log for each path evaluation step at every path evaluation interval of such attempts. As a result, you might see multiple identical messages such as `nmp_RegisterDeviceEvents failed` for device registration, which are not necessary while the device or LUN is detached.
- If you change a device configuration at runtime, changes might not be reflected in the ESXi ConfigStore that holds the configurations for an ESXi host. As a result, the datastore might not mount after the ESXi host reboots.
- Starting from ESXi 6.0, mClock is the default I/O scheduler for ESXi, but some environments might still use legacy schedulers of ESXi versions earlier than 6.0. As a result, upgrades of such hosts to ESXi 7.0 Update 3 and later might fail with a purple diagnostic screen.
- Starting with ESXi 7.0 Update 1, the configuration management of ESXi hosts moved from the `/etc/vmware/esx.conf` file to the ConfigStore framework, which makes an explicit segregation of state and configuration. Tokens in the `esx.conf` file such as `implicit_support` or `explicit_support` that indicate a state, are not recognized as valid tokens, and are ignored by the `satp_alua` module. As a result, when you upgrade ESXi hosts to ESXi 7.0 Update 3d or later by using a host profile with tokens indicating ALUA state, the operation might fail with a purple diagnostic screen. In the screen, you see an error such as `Failed modules: /var/lib/vmware/configmanager/upgrade/lib/postLoadStore/libupgradepsadeviceconfig.so`.
- A helper mechanism that caches FB resource allocation details working in background might accidentally stop and block FB resource allocation during I/O operations to the ESXi host. In some cases, this issue might affect other processes working on the same file and block them. As a result, the ESXi host might become unresponsive.
- vSAN File Service requires hosts to communicate with each other. File Service might incorrectly use an IP address in the witness network for inter-communication. If you have configured an isolated witness network for vSAN, the host can communicate with a witness node over the witness network, but hosts cannot communicate with each other over the witness network. Communication between hosts for vSAN File Service cannot be established.
- If an ESXi host is in a low memory state, insufficient heap allocation to a network module might cause the port bitmap to be set to `NULL`. As a result, the ESXi host might fail with a purple diagnostic screen when attempting to forward a packet.
- During object format change, some objects with old layout might get partially cleaned up, leaving the configuration in an invalid state. This problem can cause CLOMD to fail whenever it attempts to process the object during reconfiguration.

  You might see the following entries in `clomd.log` file:

  ```
  2022-10-14T16:17:26.456Z PANIC: NOT_REACHED bora/lib/vsan/vsan_config_builder.c:744
  ```

2022-10-14T16:17:26.456Z Backtrace:
2022-10-14T16:17:26.456Z Backtrace[0] 0000030b4742c6a0 rip=000000bf0c7de98f rbx=0000030b4742c6a0
rbp=0000030b4742cad0 r12=000000bf0d677788 r13=0000030b4742cae8 r14=000000bf14ce052c r15=000000bf14ce3c2c

- Windows 2012 and later use SCSI-3 reservation for resource arbitration to support Windows failover clustering (WSFC) on ESXi for cluster-across-box (CAB) configurations. However, if you configure the bus sharing of the SCSI controller on that VM to `Physical`, the `SCSI RESERVE` command causes the ESXi host to fail with a purple diagnostic screen. `SCSI RESERVE` is SCSI-2 semantic and is not supported with WSFC clusters on ESXi.
- vSAN might stop destaging data due to a counting issue of outstanding I/Os. If a VSAN disk group stops destaging data from the cache to the capacity tier, this can cause data to accumulate in the cache tier. This problem leads to congestion, I/O throttling, and longer latency.
- If a vSAN cluster with a 0-byte object receives a policy change request, the Cluster Level Object Manager (CLOM) might incorrectly set an invalid flag for one or more components of the object. Such a flag can cause the host to send large writes that overload the system and cause the host to fail with a purple diagnostic screen.
- A rare issue with processing VMFS journal blocks might cause lock contention that results in delays of VMFS rescan operations or failed mounting of datastores. In the vmkernel logs, you see errors such as `Resource file for resource: 6 reached max limit 8192` and `Resource file extension ('No space left on device')`.
- In rare cases, the vmx service might fail during the cancellation of a vSphere Storage vMotion task. As a result, if your environment uses vCenter Server High Availability, the service restarts the affected virtual machines.
- When you use setups with only SD or USB devices to boot ESXi 7.x, you might see errors such as `support for SD-Card/USB only configuration is being deprecated`. This message does not indicate an error, but only a warning that SD and USB devices are supported only for bootbank partitions, and for best performance, a secondary persistent storage with a minimum of 32 GB must be provided for the `/scratch` and VMware Tools which reside in the OSData partition.
- This issue applies to vSAN hosts that use an external KMS for data-at-rest encryption. When you upgrade a vSAN host from 6.7 or earlier to 7.0 and later, the KMS password is lost. The host's disks remain encrypted and locked.
- In rare cases, vSphere Virtual Volumes might attempt to rebind volumes on ESXi hosts that have SCSI Persistent Reservations. As a result, the ESXi hosts fail with a purple diagnostic screen and an error such as `Panic Message: @BlueScreen: PANIC bora/vmkernel/main/dlmalloc.c:4933 - Usage error in dlmalloc` in the backtrace.
- Due to a caching issue, in the vSphere Client you might see a VMDK size of 0 KB regardless of the actual size of virtual machines in a vSphere Virtual Volumes environment.
- During the storage migration part of a cross site Advanced Cross vCenter vMotion operation, some async I/Os at the storage stack might be trapped and not properly time out. As a result, virtual machines remain waiting for a I/O response, which causes the Advanced Cross vCenter vMotion operation to time out and the virtual machines to become unresponsive.
- A problem during LLOG recovery can cause a vSAN component to be erroneously marked as invalid. This issue can lead to log build up and congestion.
- Due to insufficient resource pool allocation, some services that report to the SFCBD, such as sfcb-vmware_base and sfcb-vmw, might fail and generate zdump. In the `syslog.log` file you see errors such as:
  `sfcb-vmware_base[2110110]: tool_mm_realloc_or_die: memory re-allocation failed(orig=364000 new=364800 msg=Cannot allocate memory, aborting`
  `sfcb-vmw_ipmi[2291550]: tool_mm_realloc_or_die: memory re-allocation failed(orig=909200 new=909600 msg=Cannot allocate memory, aborting`
- If the target policy is Raid 1, StripeWidth 1, when a vSAN cluster runs low on transient capacity, the Cluster Level Object Manager might keep reconfiguring the same part of objects larger than 8TB. As a result, such objects remain in noncompliant state, and you might see some unnecessary resync operations.
- In VMware Aria Operations for Logs, formerly vRealize Log Insight, you might see a large volume of logs generated by Storage I/O Control such as `Invalid share value: 0. Using default.` and `Skipping device naa.xxxx either due to VSI read error or abnormal state`. The volume of logs varies depending on the number of ESXi hosts in a cluster and the number of devices in switched off state. When the issue occurs, the log volume generates quickly, within 24 hours, and VMware Aria Operations for Logs might classify the messages as critical. However, such logs are harmless and do not impact the operations on other datastores that are online.
- If the storage sensor list of an ESXi host is empty, the CPU status that the Intelligent Platform Management Interface (IPMI) reports might reset. As a result, you see the sensor data record with `entity ID 3`, which is the status of the processor, displayed incorrectly as `Cannot report on the current status of the physical element` in the MOB.
- In stretch clusters, vSAN deploys each VMDK object with a specific format. When you change the policy of a VMDK object from `hostFailuresToTolerate=0` to `hostFailuresToTolerate=1`, the format might change in such a way that it can cause reads to transit the inter-site(cross-AZ) link. As a result, you see higher read latency in such objects.
- In the vSphere Client, when you create or reconfigure a virtual machine, under **SCSI controller** > **SCSI Bus Sharing** you might see doubling options in the drop-down menu. The issue does not affect any of the VM create or configure workflows.
- After a migration operation, Windows 10 virtual machines might fail with a blue diagnostic screen and report a microcode revision mismatch error such as:- `MICROCODE_REVISION_MISMATCH (17e).` The issue occurs when a scan of the CPUs runs during the migration operation and the firmware of the source CPUs does not match with the firmware of the destination CPUs.

- In certain cases, clearing the cache of objects in a datastore volume on ESXi hosts fails, objects remain in the cache, and cause out of memory state. For example, when connection with the underlying device of the volume drops. As a result, the ESXi host becomes unresponsive. In the logs, you see errors such as:
  `Cannot reconnect to xxxxx] or Failed to cleanup VMFS heartbeat on volume xxxxx: No connection.` or
  `The volume on the device xxxxx locked, possibly because some remote host encountered an error during a volume operation and could not recover.`
- Certain workflows like backup operations of ESXi hosts can open a large number of files which in turn could lead to object cache exhaustion. In such cases, you might see the hostd service to fail, or virtual machines to shut down, or the VM to get into an invalid state that prevents it to power-on. In the logs, you see warnings such as `Cannot allocate memory`.
- In **Monitor** > **Skyline Health** > **File Service** > **File Server Health**, you might see the error `File server is (re)starting`.
  The issue is caused by a cache overrun, which leads to failure of the VDFS daemon. In the `/var/run/log/vdfsd-server.log` file in an affected ESXi host, you see messages such as `NOT_IMPLEMENTED bora/vdfs/core/VDFSPhysicalLog.cpp`.
- In the vSphere Client, when you change the policy of a powered-on VM with an IDE controller, you might see the error `The attempted operation cannot be performed in the current state ("Powered on")`.
- HCI Mesh cluster mount might fail after you deactivate vSAN with data-in-transit encryption, and then reenable vSAN.
- If NVMe drives used for vSAN have a duplicate PCI ID, and you restart the vSAN health service on vCenter Server, the Hardware Compatibility group is missing from vSAN Skyline Health.
- 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.
- TPM 2.0 attestation on Lenovo servers returns the TPM error code: `TSS2_SYS_RC_INSUFFICIENT_BUFFER`.

ESXi-7.0U3i-20842708-no-tools

Profile Name	ESXi-7.0U3i-20842708-no-tools
Build	For build information, see Patches Contained in this Release.
Vendor	VMware, Inc.
Release Date	December 8, 2022
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_esx-xserver_7.0.3-0.65.20842708 • VMware_bootbank_gc_7.0.3-0.65.20842708 • VMware_bootbank_vsan_7.0.3-0.65.20842708 • VMware_bootbank_cpu-microcode_7.0.3-0.65.20842708 • VMware_bootbank_crx_7.0.3-0.65.20842708 • VMware_bootbank_esx-base_7.0.3-0.65.20842708 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.65.20842708 • VMware_bootbank_vsanhealth_7.0.3-0.65.20842708 • VMware_bootbank_native-misc-drivers_7.0.3-0.65.20842708 • VMware_bootbank_esx-ui_2.1.1-20188605 • VMware_bootbank_trx_7.0.3-0.65.20842708 • VMware_bootbank_bmcal_7.0.3-0.65.20842708 • VMware_bootbank_vdfs_7.0.3-0.65.20842708 • VMware_bootbank_esxio-combiner_7.0.3-0.65.20842708 • VMware_bootbank_esx-update_7.0.3-0.65.20842708 • VMware_bootbank_loadesx_7.0.3-0.65.20842708 • VMW_bootbank_ntg3_4.1.8.0-4vmw.703.0.65.20842708
PRs Fixed	2962719, 3021935, 2994966, 2983919, 3014323, 2996511, 2982013, 3011324, 3048788, 2983043, 3035934, 3015498, 3031708, 3041100, 3044475, 2990414, 3003866, 3011850, 3002779, 3033161, 3016132, 3015493, 3029194, 3007116, 2977496, 3021384, 2988179, 3025470, 3033159, 3011169, 3018832, 2977486, 2932056, 3013368, 2995471, 3006356, 2981272, 3000195, 3026623, 2981420, 3025469, 3042776, 2916160, 2996208, 3014374, 2977957, 2979281, 2976953, 2999968, 3031566, 3036859, 3029490, 3007883, 2992407
Related CVE numbers	N/A

- **This patch updates the following issues:**
  - Starting with 7.0 Update 2, ESXi supports Posted Interrupts (PI) on Intel CPUs for PCI passthrough devices to improve the overall system performance. In some cases, a race between PIs and the VMkernel scheduling might occur. As a result, virtual machines that are configured with PCI passthrough devices with normal or low latency sensitivity might experience soft lockups.

- 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.
- 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.
- In very rare occasions, random issues with Active Directory environments that might lead to unresponsive state of the domain controllers, might also result in unresponsiveness of the hostd service.
- 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.
- When the rhttpproxy service performs multiple operations on incoming URIs, it might miscalculate the buffer offset of each connection, which potentially leads to errors such as buffer overflows and negative reads. As a result, the service fails.
- By default, modifying hypercall options by using commands such as `vm | Get-AdvancedSetting -Name isolation.tools.autoInstall.disable` works only when the VM is powered off. For powered on VMs such calls trigger the error `The attempted operation cannot be performed in the current state (Powered on).` This is expected.
- After you update an ESXi 7.0 Update 3c host to a later version of 7.0.x or install or remove an ESXi 7.0 Update 3c VIB and reboot the host, you might see all security advanced options on the host revert to their default values. The affected advanced settings are:
  Security.AccountLockFailures
  Security.AccountUnlockTime
  Security.PasswordQualityControl
  Security.PasswordHistory
  Security.PasswordMaxDays
  Security.SshSessionLimit
  Security.DefaultShellAccess
- The command `esxcli hardware pci list`, which reports the NUMA node for ESXi host devices, returns the correct NUMA node for the Physical Functions (PF) of an SR-IOV device, but returns zero for its Virtual Functions (VF).
- After an upgrade to ESXi 7.0 Update 2 or later, when you migrate Windows virtual machines to the upgraded hosts by using vSphere vMotion, some VMs might fail with a blue diagnostic screen after the migration. In the screen, you see the error `OS failed to boot with no operating system found`. The issue occurs due to a fault in the address optimization logic of the Virtual Machine File System (VMFS).
- If the client application has no registered default request handler, requests with a path that is not present in the handler map might cause the execution of `vmacore.dll` to fail. As a result, you see the ESXi host as disconnected from the vCenter Server system.
- Some allocation reservation operations might go over the limit of 128 parallel reservation keys and exceed the allocated memory range of an ESXi host. As a result, ESXi hosts might fail with a purple diagnostic screen during resource allocation reservation operations. In the error screen, you see messages such as `PSOD BlueScreen: #PF Exception 14 in world 2097700:SCSI period IP`.
- If you run an unclaim command on a device or path while virtual machines on the device still have active I/Os, the ESXi host might fail with a purple diagnostic screen. In the screen, you see a message such as `PSOD at bora/modules/vmkernel/nmp/nmp_misc.c:3839 during load/unload of lpfc.`
- When TXT is enabled on an ESX host, attempts to power-on a VM might fail with an error. In the vSphere Client, you see a message such as `This host supports Intel VT-x, but Intel VT-x is restricted. Intel VT-x might be restricted because 'trusted execution' has been enabled in the BIOS/firmware settings or because the host has not been power-cycled since changing this setting`.
- Due to a rare issue with handling AVX2 instructions, a virtual machine of version ESX 7.0 Update 3f might fail with ESX unrecoverable error. In the `vmware.log` file, you see a message such as: `MONITOR PANIC: vcpu-0:VMM fault 6: src=MONITOR ....`
  The issue is specific for virtual machines with hardware versions 12 or earlier.
- If you use an ESXi `.iso` image created by using the Image Builder to make a vSphere Lifecycle Manager upgrade baseline for ESXi hosts, upgrades by using such baselines might fail. In the vSphere Client, you see an error such as `Cannot execute upgrade script on host`. On the impacted ESXi host, in the `/var/log/vua*.log` file, you see an error such as `ValueError: Should have base image when an addon exists`.
  The error occurs when the existing image of the ESXi host has an add-on, but the Image Builder-generated ISO provides no add-on.
- Many parallel requests for memory regions by virtual machines using the Data Plane Development Kit (DPDK) on an ESXi host might exceed the XMAP memory space on the host. As a result, the host fails with a purple diagnostic screen and an error such as: `Panic Message: @BlueScreen: VERIFY bora/vmkernel/hardware/pci/config.c:157.`
- After an upgrade of ESXi hosts to ESXi 7.0 Update 3 and later, you might no longer see some performance reports for virtual machines with NVMe controllers. For example, you do not see the Virtual Disk - Aggregate of all Instances chart in the VMware Aria Operations.
- In rare cases, such as scheduled reboot of the primary VM with FT encryption that runs heavy workloads, the secondary VM might not have sufficient buffer to decrypt more than 512 MB of dirty pages in a single FT checkpoint and experience a buffer overflow error. As a result, the ESXi host on which the secondary VM resides might fail with a purple diagnostic screen.

- In rare cases, after upgrade or update to ESXi 7.0 Update 2 and later, the vSAN storage configuration might lose the tag `mark_ssd` and default to HDD.
- Even when a device or LUN is in a detached state, the Pluggable Storage Architecture (PSA) might still attempt to register the object. PSA files a log for each path evaluation step at every path evaluation interval of such attempts. As a result, you might see multiple identical messages such as `nmp_RegisterDeviceEvents failed` for device registration, which are not necessary while the device or LUN is detached.
- If you change a device configuration at runtime, changes might not be reflected in the ESXi ConfigStore that holds the configurations for an ESXi host. As a result, the datastore might not mount after the ESXi host reboots.
- Starting from ESXi 6.0, mClock is the default I/O scheduler for ESXi, but some environments might still use legacy schedulers of ESXi versions earlier than 6.0. As a result, upgrades of such hosts to ESXi 7.0 Update 3 and later might fail with a purple diagnostic screen.
- Starting with ESXi 7.0 Update 1, the configuration management of ESXi hosts moved from the `/etc/vmware/esx.conf` file to the ConfigStore framework, which makes an explicit segregation of state and configuration. Tokens in the `esx.conf` file such as `implicit_support` or `explicit_support` that indicate a state, are not recognized as valid tokens, and are ignored by the `satp_alua` module. As a result, when you upgrade ESXi hosts to ESXi 7.0 Update 3d or later by using a host profile with tokens indicating ALUA state, the operation might fail with a purple diagnostic screen. In the screen, you see an error such as `Failed modules: /var/lib/vmware/configmanager/upgrade/lib/postLoadStore/libupgradepsadeviceconfig.so`.
- A helper mechanism that caches FB resource allocation details working in background might accidentally stop and block FB resource allocation during I/O operations to the ESXi host. In some cases, this issue might affect other processes working on the same file and block them. As a result, the ESXi host might become unresponsive.
- vSAN File Service requires hosts to communicate with each other. File Service might incorrectly use an IP address in the witness network for inter-communication. If you have configured an isolated witness network for vSAN, the host can communicate with a witness node over the witness network, but hosts cannot communicate with each other over the witness network. Communication between hosts for vSAN File Service cannot be established.
- If an ESXi host is in a low memory state, insufficient heap allocation to a network module might cause the port bitmap to be set to `NULL`. As a result, the ESXi host might fail with a purple diagnostic screen when attempting to forward a packet.
- During object format change, some objects with old layout might get partially cleaned up, leaving the configuration in an invalid state. This problem can cause CLOMD to fail whenever it attempts to process the object during reconfiguration.

  You might see the following entries in `clomd.log` file:

  ```
  2022-10-14T16:17:26.456Z PANIC: NOT_REACHED bora/lib/vsan/vsan_config_builder.c:744
  2022-10-14T16:17:26.456Z Backtrace:
  2022-10-14T16:17:26.456Z Backtrace[0] 0000030b4742c6a0 rip=000000bf0c7de98f rbx=0000030b4742c6a0
  rbp=0000030b4742cad0 r12=000000bf0d677788 r13=0000030b4742cae8 r14=000000bf14ce052c r15=000000bf14ce3c2c
  ```
- Windows 2012 and later use SCSI-3 reservation for resource arbitration to support Windows failover clustering (WSFC) on ESXi for cluster-across-box (CAB) configurations. However, if you configure the bus sharing of the SCSI controller on that VM to `Physical`, the `SCSI RESERVE` command causes the ESXi host to fail with a purple diagnostic screen. `SCSI RESERVE` is SCSI-2 semantic and is not supported with WSFC clusters on ESXi.
- vSAN might stop destaging data due to a counting issue of outstanding I/Os. If a VSAN disk group stops destaging data from the cache to the capacity tier, this can cause data to accumulate in the cache tier. This problem leads to congestion, I/O throttling, and longer latency.
- If a vSAN cluster with a 0-byte object receives a policy change request, the Cluster Level Object Manager (CLOM) might incorrectly set an invalid flag for one or more components of the object. Such a flag can cause the host to send large writes that overload the system and cause the host to fail with a purple diagnostic screen.
- A rare issue with processing VMFS journal blocks might cause lock contention that results in delays of VMFS rescan operations or failed mounting of datastores. In the vmkernel logs, you see errors such as `Resource file for resource: 6 reached max limit 8192` and `Resource file extension ('No space left on device')`.
- In rare cases, the vmx service might fail during the cancellation of a vSphere Storage vMotion task. As a result, if your environment uses vCenter Server High Availability, the service restarts the affected virtual machines.
- When you use setups with only SD or USB devices to boot ESXi 7.x, you might see errors such as `support for SD-Card/USB only configuration is being deprecated`. This message does not indicate an error, but only a warning that SD and USB devices are supported only for bootbank partitions, and for best performance, a secondary persistent storage with a minimum of 32 GB must be provided for the `/scratch` and VMware Tools which reside in the OSData partition.
- This issue applies to vSAN hosts that use an external KMS for data-at-rest encryption. When you upgrade a vSAN host from 6.7 or earlier to 7.0 and later, the KMS password is lost. The host's disks remain encrypted and locked.
- In rare cases, vSphere Virtual Volumes might attempt to rebind volumes on ESXi hosts that have SCSI Persistent Reservations. As a result, the ESXi hosts fail with a purple diagnostic screen and an error such as `Panic Message: @BlueScreen: PANIC bora/vmkernel/main/dlmalloc.c:4933 - Usage error in dlmalloc` in the backtrace.
- Due to a caching issue, in the vSphere Client you might see a VMDK size of 0 KB regardless of the actual size of virtual machines in a vSphere Virtual Volumes environment.

- During the storage migration part of a cross site Advanced Cross vCenter vMotion operation, some async I/Os at the storage stack might be trapped and not properly time out. As a result, virtual machines remain waiting for a I/O response, which causes the Advanced Cross vCenter vMotion operation to time out and the virtual machines to become unresponsive.
- A problem during LLOG recovery can cause a vSAN component to be erroneously marked as invalid. This issue can lead to log build up and congestion.
- Due to insufficient resource pool allocation, some services that report to the SFCBD, such as sfcb-vmware_base and sfcb-vmw, might fail and generate zdump. In the `syslog.log` file you see errors such as:
  `sfcb-vmware_base[2110110]: tool_mm_realloc_or_die: memory re-allocation failed(orig=364000 new=364800 msg=Cannot allocate memory, aborting`
  `sfcb-vmw_ipmi[2291550]: tool_mm_realloc_or_die: memory re-allocation failed(orig=909200 new=909600 msg=Cannot allocate memory, aborting`
- If the target policy is Raid 1, StripeWidth 1, when a vSAN cluster runs low on transient capacity, the Cluster Level Object Manager might keep reconfiguring the same part of objects larger than 8TB. As a result, such objects remain in noncompliant state, and you might see some unnecessary resync operations.
- In VMware Aria Operations for Logs, formerly vRealize Log Insight, you might see a large volume of logs generated by Storage I/O Control such as `Invalid share value: 0. Using default.` and `Skipping device naa.xxxx either due to VSI read error or abnormal state`. The volume of logs varies depending on the number of ESXi hosts in a cluster and the number of devices in switched off state. When the issue occurs, the log volume generates quickly, within 24 hours, and VMware Aria Operations for Logs might classify the messages as critical. However, such logs are harmless and do not impact the operations on other datastores that are online.
- If the storage sensor list of an ESXi host is empty, the CPU status that the Intelligent Platform Management Interface (IPMI) reports might reset. As a result, you see the sensor data record with `entity ID 3`, which is the status of the processor, displayed incorrectly as `Cannot report on the current status of the physical element` in the MOB.
- In stretch clusters, vSAN deploys each VMDK object with a specific format. When you change the policy of a VMDK object from `hostFailuresToTolerate=0` to `hostFailuresToTolerate=1`, the format might change in such a way that it can cause reads to transit the inter-site(cross-AZ) link. As a result, you see higher read latency in such objects.
- In the vSphere Client, when you create or reconfigure a virtual machine, under **SCSI controller** > **SCSI Bus Sharing** you might see doubling options in the drop-down menu. The issue does not affect any of the VM create or configure workflows.
- After a migration operation, Windows 10 virtual machines might fail with a blue diagnostic screen and report a microcode revision mismatch error such as:- `MICROCODE_REVISION_MISMATCH (17e).` The issue occurs when a scan of the CPUs runs during the migration operation and the firmware of the source CPUs does not match with the firmware of the destination CPUs.
- In certain cases, clearing the cache of objects in a datastore volume on ESXi hosts fails, objects remain in the cache, and cause out of memory state. For example, when connection with the underlying device of the volume drops. As a result, the ESXi host becomes unresponsive. In the logs, you see errors such as:
  `Cannot reconnect to xxxxx] or Failed to cleanup VMFS heartbeat on volume xxxxx: No connection.` or
  `The volume on the device xxxxx locked, possibly because some remote host encountered an error during a volume operation and could not recover.`
- Certain workflows like backup operations of ESXi hosts can open a large number of files which in turn could lead to object cache exhaustion. In such cases, you might see the hostd service to fail, or virtual machines to shut down, or the VM to get into an invalid state that prevents it to power-on. In the logs, you see warnings such as `Cannot allocate memory`.
- In **Monitor** > **Skyline Health** > **File Service** > **File Server Health**, you might see the error `File server is (re)starting`.
  The issue is caused by a cache overrun, which leads to failure of the VDFS daemon. In the `/var/run/log/vdfsd-server.log` file in an affected ESXi host, you see messages such as `NOT_IMPLEMENTED bora/vdfs/core/VDFSPhysicalLog.cpp`.
- In the vSphere Client, when you change the policy of a powered-on VM with an IDE controller, you might see the error `The attempted operation cannot be performed in the current state ("Powered on")`.
- HCI Mesh cluster mount might fail after you deactivate vSAN with data-in-transit encryption, and then reenable vSAN.
- If NVMe drives used for vSAN have a duplicate PCI ID, and you restart the vSAN health service on vCenter Server, the Hardware Compatibility group is missing from vSAN Skyline Health.
- 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.
- TPM 2.0 attestation on Lenovo servers returns the TPM error code: `TSS2_SYS_RC_INSUFFICIENT_BUFFER`.

ESXi-7.0U3si-20841705-standard

Profile Name	ESXi-7.0U3si-20841705-standard
Build	For build information, see Patches Contained in this Release.
Vendor	VMware, Inc.
Release Date	December 8, 2022
Acceptance Level	PartnerSupported

Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_esx-base_7.0.3-0.60.20841705 • VMware_bootbank_trx_7.0.3-0.60.20841705 • VMware_bootbank_vsanhealth_7.0.3-0.60.20841705 • VMware_bootbank_cpu-microcode_7.0.3-0.60.20841705 • VMware_bootbank_crx_7.0.3-0.60.20841705 • VMware_bootbank_vsan_7.0.3-0.60.20841705 • VMware_bootbank_native-misc-drivers_7.0.3-0.60.20841705 • VMware_bootbank_esx-xserver_7.0.3-0.60.20841705 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.60.20841705 • VMware_bootbank_gc_7.0.3-0.60.20841705 • VMware_bootbank_esx-ui_2.1.1-20188605 • VMware_bootbank_vdfs_7.0.3-0.60.20841705 • VMware_bootbank_bmcal_7.0.3-0.60.20841705 • VMware_bootbank_esxio-combiner_7.0.3-0.60.20841705 • VMware_bootbank_loadesx_7.0.3-0.60.20841705 • VMware_bootbank_esx-update_7.0.3-0.60.20841705 • VMware_locker_tools-light_12.1.0.20219665-20841705
PRs Fixed	2993721, 3007957, 3007958, 3015560, 3034286, 3038621, 3030691, 3015499
Related CVE numbers	CVE-2020-28196, CVE-2022-31696, CVE-2022-31699

- **This patch updates the following issues:**
  - **The cpu-microcode VIB includes the following Intel microcode:**

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Nehalem EP	0x106a5 (06/1a/5)	0x03	0x0000001d	5/11/2018	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Clarkdale	0x20652 (06/25/2)	0x12	0x00000011	5/8/2018	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series
Arrandale	0x20655 (06/25/5)	0x92	0x00000007	4/23/2018	Intel Core i7-620LE Processor
Sandy Bridge DT	0x206a7 (06/2a/7)	0x12	0x0000002f	2/17/2019	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2 (06/2c/2)	0x03	0x0000001f	5/8/2018	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d6 (06/2d/6)	0x6d	0x00000621	3/4/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Sandy Bridge EP	0x206d7 (06/2d/7)	0x6d	0x0000071a	3/24/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6 (06/2e/6)	0x04	0x0000000d	5/15/2018	Intel Xeon 65xx Series; Intel Xeon 75xx Series
Westmere EX	0x206f2 (06/2f/2)	0x05	0x0000003b	5/16/2018	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9 (06/3a/9)	0x12	0x00000021	2/13/2019	Intel i3-3200 Series; Intel i7-3500-LE/UE; Intel i7-3600-QE; Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Haswell DT	0x306c3 (06/3c/3)	0x32	0x00000028	11/12/2019	Intel Xeon E3-1200-v3 Series; Intel i7-4700-EQ Series; Intel i5-4500-TE Series; Intel i3-4300 Series
Ivy Bridge EP	0x306e4 (06/3e/4)	0xed	0x0000042e	3/14/2019	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-1600-v2 Series; Intel Xeon E5-1400-v2 Series
Ivy Bridge EX	0x306e7 (06/3e/7)	0xed	0x00000715	3/14/2019	Intel Xeon E7-8800/4800/2800-v2 Series
Haswell EP	0x306f2 (06/3f/2)	0x6f	0x00000049	8/11/2021	Intel Xeon E5-4600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-1400-v3 Series
Haswell EX	0x306f4 (06/3f/4)	0x80	0x0000001a	5/24/2021	Intel Xeon E7-8800/4800-v3 Series
Broadwell H	0x40671 (06/47/1)	0x22	0x00000022	11/12/2019	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8 (06/4d/8)	0x01	0x0000012d	9/16/2019	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series
Broadwell EP/EX	0x406f1 (06/4f/1)	0xef	0x0b000040	5/19/2021	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series
Skylake SP	0x50654 (06/55/4)	0xb7	0x02006e05	3/8/2022	Intel Xeon Platinum 8100 Series; Intel Xeon Gold 6100/5100, Silver 4100, Bronze 3100 Series; Intel Xeon D-2100 Series; Intel Xeon D-1600 Series; Intel Xeon W-3100 Series; Intel Xeon W-2100 Series
Cascade Lake B-0	0x50656 (06/55/6)	0xbf	0x04003302	12/10/2021	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/Bronze 3200; Intel Xeon W-3200
Cascade Lake	0x50657 (06/55/7)	0xbf	0x05003302	12/10/2021	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/Bronze 3200; Intel Xeon W-3200
Cooper Lake	0x5065b (06/55/b)	0xbf	0x07002501	11/19/2021	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Broadwell DE	0x50662 (06/56/2)	0x10	0x0000001c	6/17/2019	Intel Xeon D-1500 Series
Broadwell DE	0x50663 (06/56/3)	0x10	0x0700001c	6/12/2021	Intel Xeon D-1500 Series
Broadwell DE	0x50664 (06/56/4)	0x10	0x0f00001a	6/12/2021	Intel Xeon D-1500 Series
Broadwell NS	0x50665 (06/56/5)	0x10	0x0e000014	9/18/2021	Intel Xeon D-1600 Series
Skylake H/S	0x506e3 (06/5e/3)	0x36	0x000000f0	11/12/2021	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Denverton	0x506f1 (06/5f/1)	0x01	0x00000038	12/2/2021	Intel Atom C3000 Series
Ice Lake SP	0x606a6 (06/6a/6)	0x87	0x0d000375	4/7/2022	Intel Xeon Silver 4300 Series; Intel Xeon Gold 6300/5300 Series; Intel Xeon Platinum 8300 Series
Ice Lake D	0x606c1 (06/6c/1)	0x10	0x010001f0	6/24/2022	Intel Xeon D Series
Snow Ridge	0x80665 (06/86/5)	0x01	0x4c000020	5/10/2022	Intel Atom P5000 Series
Snow Ridge	0x80667 (06/86/7)	0x01	0x4c000020	5/10/2022	Intel Atom P5000 Series
Kaby Lake H/S/X	0x906e9 (06/9e/9)	0x2a	0x000000f0	11/12/2021	Intel Xeon E3-1200-v6 Series; Intel Xeon E3-1500-v6 Series
Coffee Lake	0x906ea (06/9e/a)	0x22	0x000000f0	11/15/2021	Intel Xeon E-2100 Series; Intel Xeon E-2200 Series (4 or 6 core)
Coffee Lake	0x906eb (06/9e/b)	0x02	0x000000f0	11/12/2021	Intel Xeon E-2100 Series
Coffee Lake	0x906ec (06/9e/c)	0x22	0x000000f0	11/15/2021	Intel Xeon E-2100 Series
Coffee Lake Refresh	0x906ed (06/9e/d)	0x22	0x000000f4	7/31/2022	Intel Xeon E-2200 Series (8 core)
Rocket Lake S	0xa0671 (06/a7/1)	0x02	0x00000056	8/2/2022	Intel Xeon E-2300 Series

- **ESXi 7.0 Update 3i provides the following security updates:**
  - OpenSSL is updated to version 1.0.2zf.
  - Apache Thrift is updated to version 0.15.0.
  - The urllib3 client is updated to version 1.26.5.
  - cURL is updated to version 7.84.0.
  - The SQLite database is updated to version 3.39.2.
  - The Expat XML parser is updated to version 2.4.9.
- This release resolves CVE-2022-31696, and CVE-2022-31699. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2022-0030.

- **The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3i:**
  - `windows.iso`: VMware Tools 12.1.0 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
  - `linux.iso`: VMware Tools 10.3.25 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 12.1.0 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-7.0U3si-20841705-no-tools

Profile Name	ESXi-7.0U3si-20841705-no-tools
Build	For build information, see Patches Contained in this Release.
Vendor	VMware, Inc.
Release Date	December 8, 2022
Acceptance Level	PartnerSupported
Affected Hardware	N/A
Affected Software	N/A
Affected VIBs	• VMware_bootbank_esx-base_7.0.3-0.60.20841705 • VMware_bootbank_trx_7.0.3-0.60.20841705 • VMware_bootbank_vsanhealth_7.0.3-0.60.20841705 • VMware_bootbank_cpu-microcode_7.0.3-0.60.20841705 • VMware_bootbank_crx_7.0.3-0.60.20841705 • VMware_bootbank_vsan_7.0.3-0.60.20841705 • VMware_bootbank_native-misc-drivers_7.0.3-0.60.20841705 • VMware_bootbank_esx-xserver_7.0.3-0.60.20841705 • VMware_bootbank_esx-dvfilter-generic-fastpath_7.0.3-0.60.20841705 • VMware_bootbank_gc_7.0.3-0.60.20841705 • VMware_bootbank_esx-ui_2.1.1-20188605 • VMware_bootbank_vdfs_7.0.3-0.60.20841705 • VMware_bootbank_bmcal_7.0.3-0.60.20841705 • VMware_bootbank_esxio-combiner_7.0.3-0.60.20841705 • VMware_bootbank_loadesx_7.0.3-0.60.20841705 • VMware_bootbank_esx-update_7.0.3-0.60.20841705
PRs Fixed	2993721, 3007957, 3007958, 3015560, 3034286, 3038621, 3030691
Related CVE numbers	CVE-2020-28196, CVE-2022-31696, CVE-2022-31699

- **This patch updates the following issues:**
  - **The cpu-microcode VIB includes the following Intel microcode:**

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Nehalem EP	0x106a5 (06/1a/5)	0x03	0x0000001d	5/11/2018	Intel Xeon 35xx Series; Intel Xeon 55xx Series
Clarkdale	0x20652 (06/25/2)	0x12	0x00000011	5/8/2018	Intel i3/i5 Clarkdale Series; Intel Xeon 34xx Clarkdale Series
Arrandale	0x20655 (06/25/5)	0x92	0x00000007	4/23/2018	Intel Core i7-620LE Processor
Sandy Bridge DT	0x206a7 (06/2a/7)	0x12	0x0000002f	2/17/2019	Intel Xeon E3-1100 Series; Intel Xeon E3-1200 Series; Intel i7-2655-LE Series; Intel i3-2100 Series
Westmere EP	0x206c2 (06/2c/2)	0x03	0x0000001f	5/8/2018	Intel Xeon 56xx Series; Intel Xeon 36xx Series
Sandy Bridge EP	0x206d6 (06/2d/6)	0x6d	0x00000621	3/4/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Sandy Bridge EP	0x206d7 (06/2d/7)	0x6d	0x0000071a	3/24/2020	Intel Pentium 1400 Series; Intel Xeon E5-1400 Series; Intel Xeon E5-1600 Series; Intel Xeon E5-2400 Series; Intel Xeon E5-2600 Series; Intel Xeon E5-4600 Series
Nehalem EX	0x206e6 (06/2e/6)	0x04	0x0000000d	5/15/2018	Intel Xeon 65xx Series; Intel Xeon 75xx Series
Westmere EX	0x206f2 (06/2f/2)	0x05	0x0000003b	5/16/2018	Intel Xeon E7-8800 Series; Intel Xeon E7-4800 Series; Intel Xeon E7-2800 Series
Ivy Bridge DT	0x306a9 (06/3a/9)	0x12	0x00000021	2/13/2019	Intel i3-3200 Series; Intel i7-3500-LE/UE; Intel i7-3600-QE; Intel Xeon E3-1200-v2 Series; Intel Xeon E3-1100-C-v2 Series; Intel Pentium B925C
Haswell DT	0x306c3 (06/3c/3)	0x32	0x00000028	11/12/2019	Intel Xeon E3-1200-v3 Series; Intel i7-4700-EQ Series; Intel i5-4500-TE Series; Intel i3-4300 Series
Ivy Bridge EP	0x306e4 (06/3e/4)	0xed	0x0000042e	3/14/2019	Intel Xeon E5-4600-v2 Series; Intel Xeon E5-2600-v2 Series; Intel Xeon E5-2400-v2 Series; Intel Xeon E5-1600-v2 Series; Intel Xeon E5-1400-v2 Series
Ivy Bridge EX	0x306e7 (06/3e/7)	0xed	0x00000715	3/14/2019	Intel Xeon E7-8800/4800/2800-v2 Series
Haswell EP	0x306f2 (06/3f/2)	0x6f	0x00000049	8/11/2021	Intel Xeon E5-4600-v3 Series; Intel Xeon E5-2600-v3 Series; Intel Xeon E5-2400-v3 Series; Intel Xeon E5-1600-v3 Series; Intel Xeon E5-1400-v3 Series
Haswell EX	0x306f4 (06/3f/4)	0x80	0x0000001a	5/24/2021	Intel Xeon E7-8800/4800-v3 Series
Broadwell H	0x40671 (06/47/1)	0x22	0x00000022	11/12/2019	Intel Core i7-5700EQ; Intel Xeon E3-1200-v4 Series
Avoton	0x406d8 (06/4d/8)	0x01	0x0000012d	9/16/2019	Intel Atom C2300 Series; Intel Atom C2500 Series; Intel Atom C2700 Series
Broadwell EP/EX	0x406f1 (06/4f/1)	0xef	0x0b000040	5/19/2021	Intel Xeon E7-8800/4800-v4 Series; Intel Xeon E5-4600-v4 Series; Intel Xeon E5-2600-v4 Series; Intel Xeon E5-1600-v4 Series

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Skylake SP	0x50654 (06/55/4)	0xb7	0x02006e05	3/8/2022	Intel Xeon Platinum 8100 Series; Intel Xeon Gold 6100/5100, Silver 4100, Bronze 3100 Series; Intel Xeon D-2100 Series; Intel Xeon D-1600 Series; Intel Xeon W-3100 Series; Intel Xeon W-2100 Series
Cascade Lake B-0	0x50656 (06/55/6)	0xbf	0x04003302	12/10/2021	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/Bronze 3200; Intel Xeon W-3200
Cascade Lake	0x50657 (06/55/7)	0xbf	0x05003302	12/10/2021	Intel Xeon Platinum 9200/8200 Series; Intel Xeon Gold 6200/5200; Intel Xeon Silver 4200/Bronze 3200; Intel Xeon W-3200
Cooper Lake	0x5065b (06/55/b)	0xbf	0x07002501	11/19/2021	Intel Xeon Platinum 8300 Series; Intel Xeon Gold 6300/5300
Broadwell DE	0x50662 (06/56/2)	0x10	0x0000001c	6/17/2019	Intel Xeon D-1500 Series
Broadwell DE	0x50663 (06/56/3)	0x10	0x0700001c	6/12/2021	Intel Xeon D-1500 Series
Broadwell DE	0x50664 (06/56/4)	0x10	0x0f00001a	6/12/2021	Intel Xeon D-1500 Series
Broadwell NS	0x50665 (06/56/5)	0x10	0x0e000014	9/18/2021	Intel Xeon D-1600 Series
Skylake H/S	0x506e3 (06/5e/3)	0x36	0x000000f0	11/12/2021	Intel Xeon E3-1500-v5 Series; Intel Xeon E3-1200-v5 Series
Denverton	0x506f1 (06/5f/1)	0x01	0x00000038	12/2/2021	Intel Atom C3000 Series
Ice Lake SP	0x606a6 (06/6a/6)	0x87	0x0d000375	4/7/2022	Intel Xeon Silver 4300 Series; Intel Xeon Gold 6300/5300 Series; Intel Xeon Platinum 8300 Series
Ice Lake D	0x606c1 (06/6c/1)	0x10	0x010001f0	6/24/2022	Intel Xeon D Series
Snow Ridge	0x80665 (06/86/5)	0x01	0x4c000020	5/10/2022	Intel Atom P5000 Series
Snow Ridge	0x80667 (06/86/7)	0x01	0x4c000020	5/10/2022	Intel Atom P5000 Series
Kaby Lake H/S/X	0x906e9 (06/9e/9)	0x2a	0x000000f0	11/12/2021	Intel Xeon E3-1200-v6 Series; Intel Xeon E3-1500-v6 Series
Coffee Lake	0x906ea (06/9e/a)	0x22	0x000000f0	11/15/2021	Intel Xeon E-2100 Series; Intel Xeon E-2200 Series (4 or 6 core)
Coffee Lake	0x906eb (06/9e/b)	0x02	0x000000f0	11/12/2021	Intel Xeon E-2100 Series
Coffee Lake	0x906ec (06/9e/c)	0x22	0x000000f0	11/15/2021	Intel Xeon E-2100 Series
Coffee Lake Refresh	0x906ed (06/9e/d)	0x22	0x000000f4	7/31/2022	Intel Xeon E-2200 Series (8 core)

Code Name	FMS	Plt ID	MCU Rev	MCU Date	Brand Names
Rocket Lake S	0xa0671 (06/a7/1)	0x02	0x00000056	8/2/2022	Intel Xeon E-2300 Series

- **ESXi 7.0 Update 3i provides the following security updates:**
  - OpenSSL is updated to version 1.0.2zf.
  - Apache Thrift is updated to version 0.15.0.
  - The urllib3 client is updated to version 1.26.5.
  - cURL is updated to version 7.84.0.
  - The SQLite database is updated to version 3.39.2.
  - The Expat XML parser is updated to version 2.4.9.
- This release resolves CVE-2022-31696, and CVE-2022-31699. For more information on these vulnerabilities and their impact on VMware products, see VMSA-2022-0030.

- **The following VMware Tools ISO images are bundled with ESXi 7.0 Update 3i:**
  - `windows.iso`: VMware Tools 12.1.0 supports Windows 7 SP1 or Windows Server 2008 R2 SP1 and later.
  - `linux.iso`: VMware Tools 10.3.25 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 12.1.0 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_7.0.3-0.65.20842708

Name	ESXi
Version	ESXi_7.0.3-0.65.20842708
Release Date	December 8, 2022
Category	Bugfix
Affected Components	• ESXi Component - core ESXi VIBs • ESXi Install/Upgrade Component • Broadcom NetXtreme I ESX VMKAPI ethernet driver
PRs Fixed	
Related CVE numbers	N/A

ESXi_7.0.3-0.60.20841705

Name	ESXi
Version	ESXi_7.0.3-0.60.20841705
Release Date	December 8, 2022
Category	Security
Affected Components	• ESXi Component - core ESXi VIBs • ESXi Install/Upgrade Component • ESXi Tools Component
PRs Fixed	
Related CVE numbers	N/A

Known Issues

The known issues are grouped as follows.

Installation, Upgrade and Migration Issues

- **The vlanid property in custom installation scripts might not work**
  If you use a custom installation script that sets the `vlanid` property to specify a desired VLAN, the property might not take effect on newly installed ESXi hosts. The issue occurs only when a physical NIC is already connected to DHCP when the installation starts. The `vlanid` property works properly when you use a newly connected NIC.

  Workaround: Manually set the VLAN from the Direct Console User Interface after you boot the ESXi host. Alternatively, disable the physical NIC and then boot the host.

- **HPE servers with Trusted Platform Module (TPM) boot, but remote attestation fails**
  Some HPE servers do not have enough event log space to properly finish TPM remote attestation. As a result, the VMkernel boots, but remote attestation fails due to the truncated log.

  Workaround: None.

Known Issues from Previous Releases

To view a list of previous known issues, click here.