vcf-security-and-compliance-guidelines/security-advisories/vmsa-2025-0004 at main · vmware/vcf-security-and-compliance-guidelines

By plankers

Archived: 2026-04-05 23:40:10 UTC

VMSA-2025-0004: Questions & Answers

Introduction

On March 4, 2025 Broadcom released a critical VMware Security Advisory (VMSA), VMSA-2025-0004, addressing security vulnerabilities found and resolved in VMware ESX regarding a mechanism where threat actors could access the hypervisor through a running virtual machine.

The advisory references patches applicable to all supported versions of VMware ESX. All customers should apply these updates.

The VMSA will always be the source of truth for what products & versions are affected and proper patches to keep your organization secure. This document is a corollary to the advisory and includes self-service information to help you and your organization decide how to respond.

You are affected if you are running any version of VMware ESX, VMware vSphere, VMware Cloud Foundation, or VMware Telco Cloud Platform prior to the versions listed as “fixed” in the VMSA. Please consult the VMSA itself for the definitive list of affected versions. If you have a question about whether you are affected it is probable that you are, and should take action immediately.

If you are experiencing issues with the Broadcom Support Portal please see the section below entitled "I currently have an active entitlement however I cannot see all the fixed versions relating to the VMSA" for more information.

Current Update

Updated on March 6, 2025 at 0815 PST (-0800)

Next Expected Update

There is not a regular update schedule for this document; it will be updated as needed.

Relevant Links

VMware Security Advisory VMSA-2025-0004 (the security advisory itself)
VMSA-2025-0004 Questions & Answers (this document's shortened ink)
vSphere Security Configuration & Hardening Guides (the reference for hardening VMware vSphere, virtual machines, and in-guest settings like VMware Tools)
VMware Cloud Foundation Security Advisories (list of all disclosed security vulnerabilities)
VMware Security Advisory Mailing List (please subscribe for proactive notifications of security advisories)
VMware Ports & Protocols & VMware vSphere Firewalling Helper (assistance in determining ingress & egress firewall rule sets)
VMware vSphere Critical Patch Downloads (support.broadcom.com)

Questions & Answers

Who does this affect?

You are affected if you are running any version of VMware ESX, VMware vSphere, VMware Cloud Foundation, or VMware Telco Cloud Platform prior to the versions listed as "fixed" in the VMSA.

For a definitive list of affected versions, please refer to the VMSA directly. If there is any uncertainty about whether a system is affected, it should be presumed vulnerable, and immediate action should be taken.

When do I need to act?

These issues would qualify under ITIL methodologies as an emergency change, requiring prompt action from your organization. However, the specific response timing depends on your unique circumstances. It is advisable to consult immediately with your organization's information security staff. They will assess the situation and determine the most appropriate course of action for your specific organizational context.

What should I do to protect myself?

To ensure full protection for yourself and your organization, install one of the update versions listed in the VMware Security Advisory.

What products are affected?

VMware ESX and any products that contain ESX, including VMware vSphere, VMware Cloud Foundation, and VMware Telco Cloud Platform.

What CVE numbers are involved in these disclosures?

CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226

What is the severity of the vulnerabilities?

9.3, 8.2, and 7.1, scored using version 3.1 of the Common Vulnerability Scoring Standard (CVSS).

Are there additional details about the vectors of the vulnerabilities?

VMware Security Advisories link to the FIRST CVSS v3.1 calculator, with the vectors pre-filled for the individual vulnerabilities. This information is found in the 'References' section of the advisory.

Are the vulnerabilities being exploited "in the wild?"

Broadcom has information to suggest that exploitation of these issues has occurred "in the wild."

Is this a "VM Escape?"

Yes. This is a situation where an attacker who has already compromised a virtual machine's guest OS and gained privileged access (administrator or root) could move into the hypervisor itself.

Do I have to update VMware vCenter?

While it is recommended that vCenter be maintained at the latest patch levels, this advisory does not affect vCenter directly.

Do I have to update VMware ESX?

Yes; ESX is affected by this VMSA.

Is this patch eligible for Live Patch?

No; Although Live Patch was announced following the release of vSphere 8.0 Update 3, the nature of this particular issue prevents the use of live patching.

I currently have an active entitlement however I cannot see all the fixed versions relating to the VMSA.

To access a patch from any version, for example: 7 patch you must have a License Key of the same version to view and download. If the licenses on your site ID contain one version you will have to upgrade/downgrade licenses to access another version. For more information relating to upgrading/downgrading licenses see Upgrade and Downgrade VMware License Keys

Do I have to update SDDC Manager?

No; SDDC Manager is not affected by this VMSA.

Do I have to update VMware Cloud Foundation Operations, Automation, or Aria Suite components?

No; these components are not affected by this VMSA.

Do I have to update VMware NSX?

No; NSX is not affected by this VMSA.

Will there be a patch for VMware Cloud Foundation?

Yes, there is an asynchronous patch for supported versions of the VMware Cloud Foundation. Please follow the instructions linked in the VMSA itself.

Will there be a patch for VMware Telco Cloud Platform?

VMware Telco Cloud Platform customers will need to update to a version of ESXi that contains the fixes, which may necessitate moving to a newer version of VMware Telco Cloud Platform (TCP). For more details please consult the instructions in the VMSA itself.

Are there workarounds for these vulnerabilities?

There are no feasible workarounds for this situation.

Exploiting this vulnerability does require administrator/root privileges on a guest operating system, so there are other layers of defenses that can help if they are in place. There are no other meaningful workarounds that do not involve updating and restarting VMware ESX.

For assistance that is tailored to your environment and organization please contact your account team.

If I do not install VMware Tools am I safe?

No. An attacker with privileged access to your guest operating system can install and/or re-enable the VMware Tools for you.

Do I need to update VMware Tools?

Broadcom recommends always maintaining VMware Tools at the most recent patch levels, but you do not need to update VMware Tools specifically as part of this advisory.

What versions or builds are affected by these issues?

You are affected if you are running any version of ESX prior to the fixed versions listed in the VMSA. Please consult the VMSA itself for the definitive list of affected versions. If you have a question about whether you are affected it is likely that you are, and should take action immediately.

Broadcom always recommends applying the latest updates to all software products.

How do I check the build or version number of VMware ESX?

The build information is available in the Summary tab of the vSphere Client. It can also be easily queried with PowerCLI:

```
Get-VMhost | Select-Object Name,Version,Build
```

If I update ESX will it affect running workloads?

Broadcom recommends the use of vMotion to relocate virtual machines to alternate hosts while you update, in a “rolling reboot” fashion. Virtual machines that do not use vMotion will need to be powered down during the host restart.

Are there any known issues with this patch?

There are no known issues with the updates listed in VMSA-2025-0004.

I am amidst an upgrade of my environment. Are there any concerns with applying this patch?

This patch is a “back in time” situation, and moving from vSphere 8 Update 2d to vSphere 8 Update 3 may result in security exposures. Consult the release notes for this update for more information, and ensure that, as part of your upgrade process, you are also applying the latest patches to the upgraded environment.

Does this impact VMware vSphere 6.5 or 6.7?

Yes. A patch has been released for ESX 6.7 and is available via the Support Portal to all customers. ESX 6.5 customers should use the extended support process for access to ESX 6.5 patches.

Products that are past their End of General Support dates are not evaluated as part of security advisories, and are not listed in the official VMSA. Broadcom strongly encourages all customers using vSphere 6.5 and 6.7 to update to vSphere 8.

Do I have to update to vSphere 8 Update 3 to receive this patch?

Yes. vSphere 8 Update 3 was released in July 2024 and is considered the best version of vSphere 8, intended for long-term stability and support.

Do I have to update to vSphere 7 Update 3 to receive this patch?

Yes. vSphere 7 Update 3 was released in January 2022 and is considered the best version of vSphere 7, intended for long-term stability and support.

I am using a third-party solution such as HPE SimpliVity, Dell EMC VxRail, and so on. Is it safe for me to apply the update?

Third-party engineered systems control their patch levels and configurations as part of their qualification and testing processes. Using security guidance that is not explicitly for that product and product version is never advised. If you use engineered and integrated solutions please contact those vendors directly for guidance. Broadcom is not involved in, and cannot speak to, third-party product release schedules.

35. Are VMware Cloud and hosted products updated?

VMSA information is delivered as a message inside hosted, cloud, and software-as-a-service products where applicable. Please check the administrative consoles of those services for further relevant messages and details

about this VMSA. Additional questions about the service should be answered through the support processes for that service. Thank you.

Change Log

Specific changes to this document can be easily tracked with GitHub's "History" and "Blame" functions (buttons above).

Disclaimer

This document is intended to provide general guidance for organizations that are considering Broadcom solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided “AS IS.” Broadcom makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.
