vcf-security-and-compliance-guidelines/security-advisories/vmsa-2024-0019/README.md at main · vmware/vcf-security-and-compliance-guidelines

By plankers

Archived: 2026-04-06 03:11:36 UTC

VMSA-2024-0019: Questions & Answers

Introduction

On September 17, 2024 Broadcom released a critical VMware Security Advisory (VMSA), VMSA-2024-0019, addressing security vulnerabilities found and resolved in VMware vCenter. The advisory was updated on October 21, 2024 with updated software packages to address security and functional issues reported after the original disclosure.

The updated advisory contains patches applicable to vCenter 7.0.3, 8.0.2, and 8.0.3. All customers should apply these refreshed 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.

These vulnerabilities are memory management and corruption issues which can be used against VMware vCenter services, potentially allowing remote code execution.

You are affected if you are running any version of vSphere or VMware Cloud Foundation prior to the 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.

Current Update

Updated at 0930 PDT (-0700) on November 18, 2024.

Next Expected Update

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

Relevant Links

VMware Security Advisory VMSA-2024-0019 (the security advisory itself)

VMSA-2024-0019 Questions & Answers (this document's link)

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)

Best Practices for Patching VMware vSphere (advice for ensuring patching success)

VMware Ports & Protocols & VMware vSphere Firewalling Helper (assistance in determining ingress & egress firewall rule sets)

VMware vSphere Critical Patch Downloads (support.broadcom.com)

vSphere Web Client Becomes Unresponsive After Upgrading to vCenter 8 Update 3B (KB and workaround)

Who does this affect?

These vulnerabilities affect customers who have deployed VMware vCenter. Users of VMware vSphere or VMware Cloud Foundation running versions older than the fixed versions listed in the VMSA are vulnerable.

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.

While other mitigations may be available depending on your organization's security posture, defense-in-depth strategies, and firewall configurations, each organization must evaluate the adequacy of these protections independently.

The most reliable method to address these vulnerabilities is to apply the recommended patches.

What products are affected?

VMware vCenter and any products that contain vCenter, including VMware vSphere and VMware Cloud Foundation.

What CVE numbers are involved in these disclosures?

CVE-2024-38812 and CVE-2024-38813.

What is the severity of the vulnerabilities?

9.8 and 7.5, 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 confirmed that exploitation has occurred "in the wild" for CVE-2024-38812 and CVE-2024-38813.

If I updated with the initial patches in VMSA-2024-0019 do I need to update with VMSA-2024-0019.2?

Yes. These new updates resolve security and operational issues reported to us after the initial release.

Is the workaround still necessary for the web client issues?

No, the patches listed in VMSA-2024-0019.2 resolve the web client issues wherever they were present.

If I did the workaround for the web client issues, do I have to undo it to apply the patches?

No. Just apply the patch.

Do I have to apply both sets of patches?

Security updates are cumulative within a product branch. If you apply the latest patches for a supported version of vSphere or Cloud Foundation you will have all of the available updates.

Do I have to update VMware vCenter?

Yes; vCenter is affected by this VMSA.

See “Best Practices for Patching VMware vSphere” for guidance on updating vSphere components.

Do I have to update VMware ESXi?

No; ESXi is not affected by this VMSA.

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 or Automation 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. However, there is a recent VMSA that does impact NSX, which you should evaluate.

Will there be a patch for VMware Cloud Foundation?

Yes, there is an asynchronous patch for VMware Cloud Foundation 4.x and 5.x. Please follow the instructions linked in the VMSA itself.

There was a commitment made to provide critical patches for perpetual-license vSphere customers. How do I download those patches?

On April 15, 2024, Broadcom announced via blog post that all customers, including those with expired support contracts, will have access to all patches for Critical Severity Security Alerts for supported versions of VMware vSphere. This policy can be found in KB 314603.

These patches are located on support.broadcom.com. You will need to create an account, which can be done in a few minutes and at no cost.

1. Log in and choose “VMware Cloud Foundation” from the drop down menu near the top right.
2. Choose “My Downloads” from the menu on the left.
3. Choose “VMware vSphere” as the product (page two of the list).
4. Choose the “Solutions” tab.
5. Choose the edition and version of vSphere.

A direct link to this location is in the links above. You may need to log in first and then visit the link.

Are there workarounds for these vulnerabilities?

Not as part of this advisory. There may be other mitigations and compensating controls available in your organization, depending on your security posture, defense-in-depth strategies, and configurations of perimeter firewalls and appliance firewalls. All organizations must decide for themselves whether to rely on those protections; VMware Global Support (GS) cannot decide for you what is appropriate for your organization.

For assistance that is tailored to your environment and organization please contact your account team about VMware Professional Services.

If I am not using Enhanced Linked Mode am I safe?

No; the issues in this VMSA are not due to the use of Enhanced Linked Mode (ELM), they are issues with vCenter itself, and present even if ELM is not in use. Even if you are not using ELM you need to update or take steps to

mitigate the issues.

If I am not using Integrated Windows Authentication am I safe?

No; the issues in this VMSA are not due to the use of Integrated Windows Authentication (IWA), they are issues with vCenter itself, and present even if IWA is not in use. Even if you are not using IWA you need to update or take steps to mitigate the issues.

What versions or builds are affected by these issues?

You are affected if you are running any version of vCenter 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 vCenter?

The build information is available in the Summary tab of the vSphere Client. It can also be queried with PowerCLI. Once connected using Connect-VIServer, build information is available in the $global:DefaultVIServer.Build variable (there is also $global:DefaultVIServer.Version).

If I update vCenter will it affect running workloads?

No. vCenter is the management interface to a vSphere cluster. You will lose the use of the vSphere Client briefly during the update, and other management methods will be similarly impacted, but virtual machine and container workloads will be unaffected.

Can I use the vCenter VAMI to apply these updates?

Yes, the patch is available through the standard update mechanisms for VMware vSphere and VMware Cloud Foundation. Consult the product documentation for the version of the product you use.

See “Best Practices for Patching VMware vSphere” for additional guidance on updating vSphere components.

Are there any known issues with this patch?

There are no known issues with the updates listed in VMSA-2024-0019.2.

There was an issue with the original VMSA-2024-0019 update regarding session timeouts when accessing vCenter (with a workaround at KB 377734.. This is resolved with the re-release.

If you enable SSH on vCenter in order to implement the workaround, remember to disable it again afterwards.

Does this impact VMware vSphere 6.5 or 6.7?

Yes. Products that are past their End of General Support dates are not evaluated as part of security advisories. If your organization has extended support please use those processes to request assistance.

Do I have to update to vCenter 8.0.3 to receive this patch?

No. You can update either vCenter 8.0.2 or vCenter 8.0.3.

vSphere 8 Update 3 is considered the best version of vSphere 8 and intended for long-term stability and support. All new security updates are built atop vSphere 8 Update 3.

Do I have to update to vCenter 7.0.3 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.

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.
