THREAT BULLETINS

Multiple Vulnerabilities Affecting VMware Solutions Under Active Exploitation

TLP:WHITE

Mar 04, 2025

On March 4, 2025, Broadcom released an advisory (VMSA-2025-0004) prompted by the Microsoft Threat Intelligence Center's disclosure of multiple, actively exploited, zero-day vulnerabilities affecting VMware ESXi, Workstation, Fusion, Cloud Foundation, and Telco Cloud Platform solutions.

The vulnerabilities are tracked as CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226.

Health-ISAC provides this information for situational awareness and encourages users to upgrade affected VMware products to the latest patched versions.

The most severe of these vulnerabilities, CVE-2025-22224, has a CVSS score of 9.3 and is a Time-of-Check Time-of-Use (TOCTOU) flaw. The vulnerability can lead to an out-of-bounds write, which a threat actor with elevated privileges on a virtual machine could exploit to execute code in the virtual machine executable (VMX) process running on the host.

The second vulnerability, identified as CVE-2025-22225, has a CVSS score of 8.2 and is an arbitrary write flaw. Successful exploitation of the vulnerability allows a threat actor with privileges within the VMX process to perform a sandbox escape, bypassing limitations set

within the virtual environment to be able to interact with system resources.

The third vulnerability, tracked as CVE-2025-22226, has a CVSS score of 7.1 and is an information disclosure flaw that is caused by an out-of-bounds read in the Host Guest File System (HGFS) driver. Threat actors seeking to exploit this vulnerability could leak memory from the VMX process.

The affected product versions include:

- VMware ESXi 8.0 - Fixed in ESXi80U3d-24585383, ESXi80U2d-24585300
- VMware ESXi 7.0 - Fixed in ESXi70U3s-24585291
- VMware Workstation 17.x - Fixed in 17.6.3
- VMware Fusion 13.x - Fixed in 13.6.3
- VMware Cloud Foundation 5.x - Async patch to ESXi80U3d-24585383
- VMware Cloud Foundation 4.x - Async patch to ESXi70U3s-24585291
- VMware Telco Cloud Platform 5.x, 4.x, 3.x, 2.x - Fixed in ESXi 7.0U3s, ESXi 8.0U2d, and ESXi 8.0U3d
- VMware Telco Cloud Infrastructure 3.x, 2.x - Fixed in ESXi 7.0U3s

Recommendations:

Health-ISAC recommends organizations review and assess their level of risk to this activity and take the necessary actions to ensure appropriate security measures are implemented, including:

- Immediately applying the latest patches for affected product versions.
- Implementing the principle of least privilege to minimize potential impacts if exploitation occurs.
- Reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	Broadcom, The Hacker News, Bleeping Computer, Infosecurity Magazine, HHS

Alert ID a2f3e38f

View Alert

Share Feedback

was this helpful? |

Tags VMware Telco Cloud Platform, CVE-2025-22226, CVE-2025-22225, CVE-2025-22224, VMware Cloud Foundation, VMware ESXi, VMware Fusion, VMware Workstation

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**