Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

VMware Fixes Three Actively Exploited Zero-Days - Patch Now!

Date of Publication	Admiralty Code	TA Number
March 5, 2025	A1	TA2025065

Summary

First Seen: March 4, 2025
Affected Products: VMware ESXi, VMware Workstation Pro / Player (Workstation), VMware Fusion, VMware Cloud Foundation, VMware Telco Cloud Platform
Impact: VMware has patched three actively exploited zero-day vulnerabilities affecting its ESXi, Workstation, and Fusion products. Tracked as CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226, these flaws allow attackers with administrative or root privileges to break out of the virtual machine sandbox, potentially compromising the underlying host system.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-22224	VMware ESXi and Workstation TOCTOU Race Condition Vulnerability	VMware ESXi and Workstation	✓	✓	✓
CVE-2025-22225	VMware ESXi Arbitrary Write Vulnerability	VMware ESXi	✓	✓	✓
CVE-2025-22226	VMware ESXi, Workstation, and Fusion Information Disclosure Vulnerability	VMware ESXi, Workstation, and Fusion	✓	✓	✓

Vulnerability Details

#1 VMware has released security patches to address three actively exploited zero-day vulnerabilities - CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226 affecting ESXi, Workstation, and Fusion. These flaws could allow attackers to break out of virtual machine sandboxes, posing a significant risk to host systems.

#2 CVE-2025-22224 is a Time-of-Check Time-of-Use (TOCTOU) vulnerability affecting ESXi and Workstation. It can lead to an out-of-bounds write, enabling an attacker with local administrative privileges on a virtual machine to execute arbitrary code as the VMX process on the host system. This flaw could be leveraged to move beyond the virtual machine boundary, potentially compromising the hypervisor.

#3 CVE-2025-22225 is an arbitrary write vulnerability in ESXi, allowing an attacker with access to the VMX process to manipulate kernel memory. This could lead to a full sandbox escape, granting the attacker control over the underlying host. Such an exploit could be particularly dangerous in cloud environments and data centers where multiple virtual machines run on the same infrastructure.

#4 CVE-2025-22226 is an information disclosure vulnerability found in ESXi, Workstation, and Fusion. It results from an out-of-bounds read in the Host Guest File System (HGFS). Attackers with administrative privileges on a virtual machine could exploit this flaw to leak memory from the VMX process, potentially exposing sensitive information.

#5 These vulnerabilities can be chained together, allowing an attacker who has already compromised a virtual machine's guest OS and gained privileged access to escalate their attack and compromise the hypervisor. Given the severity of these flaws, VMware strongly advises users to upgrade to the latest patched versions of their respective products to mitigate the risk of exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-22224	VMware ESXi Versions 7.0 and 8.0, VMware Cloud Foundation Version 4.5.x and 5.x, VMware Telco Cloud Platform Version 5.x, 4.x, 3.x, and 2.x, VMware Telco Cloud Infrastructure Version 3.x and 2.x, VMware Workstation Version 17.x	cpe:2.3:o:vmware:esxi:-:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:workstation:*:*:*:*:*:*:*:*	CWE-367
CVE-2025-22225	VMware ESXi Versions 7.0 and 8.0, VMware Cloud Foundation Version 4.5.x and 5.x, VMware Telco Cloud Platform Version 5.x, 4.x, 3.x, and 2.x, VMware Telco Cloud Infrastructure Version 3.x and 2.x	cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:*	CWE-123
CVE-2025-22226	VMware ESXi Versions 7.0 and 8.0, VMware Cloud Foundation Version 4.5.x and 5.x, VMware Telco Cloud Platform Version 5.x, 4.x, 3.x, and 2.x, VMware Telco Cloud Infrastructure Version 3.x and 2.x, VMware Workstation Version 17.x, VMware Fusion Version 13.x	cpe:2.3:o:vmware:esxi:-:*:*:*:*:*:*:* cpe:2.3:a:vmware:cloud_foundation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:telco_cloud_platform:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:workstation:*:*:*:*:*:*:*:* cpe:2.3:a:vmware:fusion:*:*:*:*:*:*:*:*	CWE-125

Recommendations

Stay Updated: Ensure your VMware ESXi, Workstation, and Fusion installations are updated to the latest patched versions. These updates address critical vulnerabilities (CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226) that attackers are actively exploiting.

Limit Privileged Access: Limit administrative and root access to virtual machines to prevent attackers from exploiting vulnerabilities to break out of the VM sandbox. By restricting high-level privileges, you reduce the chances of an attacker gaining control over the hypervisor and compromising the host system.

Monitor for Suspicious Activity: Deploy security monitoring tools to detect anomalies within virtual environments, such as unauthorized login attempts, privilege escalation, or unusual interactions with the VMX process.

Strengthen Virtual Machine Security: Implement strict access controls and network segmentation to prevent attackers from moving laterally in case of a compromise. Additionally, harden virtual machine security by disabling unnecessary services, enforcing strong authentication, and following VMware's best security practices.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0004** Privilege Escalation
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1068** Exploitation for Privilege Escalation	**T1059** Command and Scripting Interpreter
T1078 Valid Accounts			

Patch Details

To address CVE-2025-22224, CVE-2025-22225 and CVE-2025-22226, users are urged to apply the latest updates immediately.

Links:
https://support.broadcom.com/web/ecx/solutiondetails?patchId=5773 ,
https://support.broadcom.com/web/ecx/solutiondetails?patchId=5772 ,
https://support.broadcom.com/web/ecx/solutiondetails?patchId=5771 ,
https://support.broadcom.com/group/ecx/productfiles?subFamily=VMware%20Workstation%20Pro&displayGroup=VMware%20Workstation%20Pro%2017.0%20for%20Windows&release=17.6.3&os=&servicePk=undefined&language=EN&freeDownloads=true ,
https://support.broadcom.com/group/ecx/productfiles?subFamily=VMware%20Fusion&displayGroup=VMware%20Fusion%2013&release=13.6.3&os=&servicePk=undefined&language=EN&freeDownloads=true ,
https://knowledge.broadcom.com/external/article?legacyId=88287 ,
https://knowledge.broadcom.com/external/article/389385

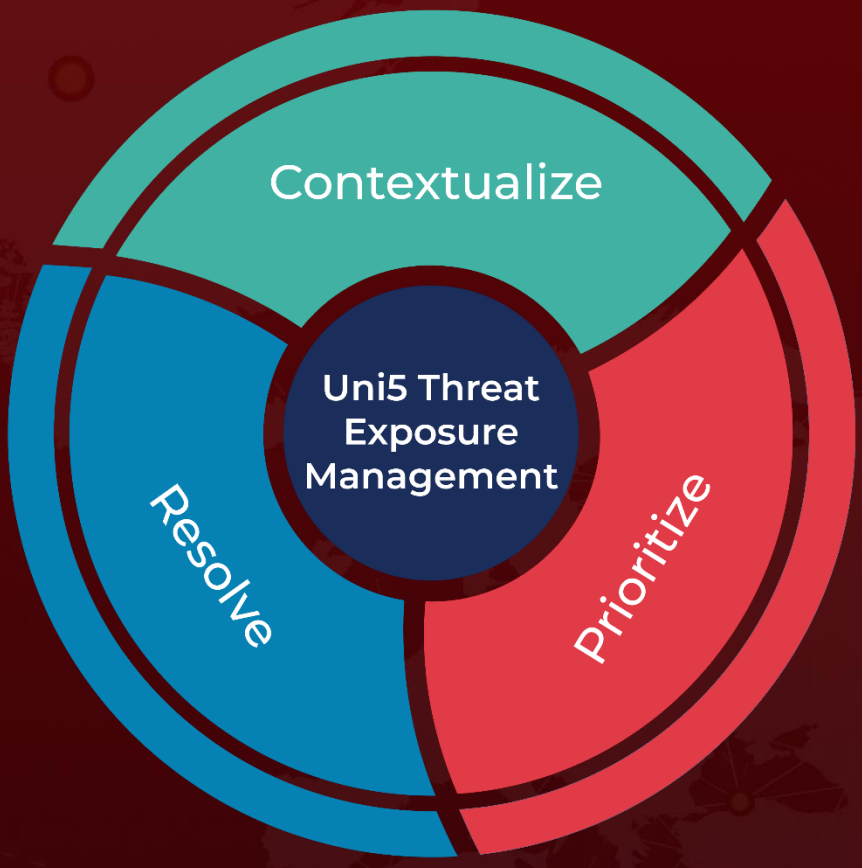
References

https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 5, 2025 • 5:00 AM

More at www.hivepro.com