Critical VMware Vulnerabilities Expose Host Systems to Malicious Code Execution

TL;DR

VMware released patches addressing four critical vulnerabilities (CVE-2025-41236, CVE-2025-41237, CVE-2025-41238, CVE-2025-41239) impacting ESXi, Workstation, Fusion, and VMware Tools.

Exploitation could allow attackers with VM admin privileges to execute code on the host or leak sensitive memory information.

Overview

VMware has issued critical security updates to fix multiple severe vulnerabilities across VMware ESXi, Workstation, Fusion, VMware Tools, VMware Cloud Foundation, and VMware Telco Cloud platforms. The vulnerabilities, with CVSS scores ranging from 6.2 to 9.3, could allow attackers to execute malicious code on host systems or leak sensitive memory data, severely compromising virtualization infrastructure.

Affected Products

- VMware Cloud Foundation (4.5.x, 5.x)
- VMware vSphere Foundation (9.0.0.0)
- VMware ESXi (7.0, 8.0)
- VMware Workstation Pro (17.x)
- VMware Fusion (13.x)
- VMware Tools (Windows versions 11.x, 12.x, 13.x)
- VMware Telco Cloud Platform (2.x, 3.x, 4.x, 5.x)
- VMware Telco Cloud Infrastructure (2.x, 3.x)

Vulnerability Breakdown

- **CVE-2025-41236** – VMXNET3 Integer Overflow (Critical, CVSS 9.3)
  This flaw affects the VMXNET3 virtual network adapter, allowing attackers with local admin privileges on a VM to execute arbitrary code on the host. It directly impacts VMware ESXi (7.0, 8.0), Workstation Pro (17.x), and Fusion (13.x).

- **CVE-2025-41237** – VMCI Integer Underflow (Critical, CVSS 9.3 Workstation/Fusion, 8.4 ESXi)
  An integer underflow in VMCI can lead to out-of-bounds writes, allowing attackers to execute code within the VM's VMX process. On ESXi, exploitation is sandboxed within VMX. However, exploitation on Workstation and Fusion can lead to full host compromise.
- **CVE-2025-41238** – PVSCSI Heap Overflow (Critical, CVSS 9.3 Workstation/Fusion, 7.4 ESXi)
  Heap overflow in the Paravirtualized SCSI controller allows attackers to execute malicious code in the VMX process context. ESXi systems are vulnerable only in unsupported configurations. Workstation and Fusion deployments face higher risk.
- **CVE-2025-41239** – vSockets Information Disclosure (Moderate, CVSS 7.1 ESXi/Workstation/Fusion, 6.2 VMware Tools)
  Use of uninitialized memory in vSockets allows attackers to leak sensitive memory data from affected systems. Primarily impacts VMware Tools for Windows (versions 11.x, 12.x, 13.x). Linux and macOS are unaffected.

Aspire Protects

- **Patch -** Deploy patches immediately
  - VMware ESXi:
    - Version 8.0 - ESXi80U3f-24784735
    - Version 7.0 - ESXi70U3w-24784741
  - VMware Workstation Pro - 17.6.4
  - VMware Fusion - 13.6.4
  - VMware Tools - 13.0.1.0 (Windows)

TTPs to Watch

Privilege Escalation

- Escape to Host [T1611] - Attackers may exploit these vulnerabilities to break out of the VM environment and execute arbitrary code directly on the host system.

Execution

- Exploitation for Client Execution [T1203] - Attackers could leverage integer overflow/underflow and heap overflow vulnerabilities to execute code via malicious VM actions.

Credential Access

- Exploitation for Credential Access [T1212] - Information disclosure vulnerability (CVE-2025-41239) may allow attackers to obtain sensitive memory data.

IoCs

There are no known IoCs associated with the above vulnerabilities at this time. All vulnerabilities were responsibly disclosed through the Pwn2Own competition and patched before public exploitation was reported. However, due to the nature of these flaws, particularly their potential for full VM escape and host-level code execution, threat actors may try to weaponize exploits soon. It's wise to monitor for:

- Unusual outbound traffic from virtual machines with VMXNET3, VMCI, or PVSCSI devices.
- Unexpected VMX process behavior on ESXi hosts.
- Unauthorized access or modification attempts on files related to VMware Tools or vSockets.
- Alerts triggered by host-based intrusion detection systems (HIDS) tied to memory manipulation or privilege escalation from guest to host.

Aspire is actively monitoring and will notify customers if any IoCs are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

Targeted Industries

Given VMware's extensive deployment, organizations in these sectors should patch as soon as possible:

- Financial Services
- Healthcare
- Technology and Cloud Providers
- Telecommunications
- Government
- Manufacturing
- Retail
- Energy and Utilities

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

Support Content Notification - Support Portal - Broadcom support portal