Multiple Vulnerabilities in VMware ESXi

Severity Level: HIGH

Components Affected

- VMware ESXi 8.0 and 7.0
- VMware Workstation 17.x
- VMware Fusion 13.x
- VMware Tools 13.x

Overview

Multiple high-severity vulnerabilities were identified in VMware products as part of the Pwn2Own Berlin 2025 event. These flaws allow attackers with administrative access inside virtual machines to potentially execute code on the host system, leading to privilege escalation and information leakage.

Description

The identified vulnerabilities include:

• CVE-2025-41236 - Integer overflow in the VMXNET3 network adapter. Allows remote code execution on the host from a compromised VM.

• CVE-2025-41237 - Integer underflow in the VMCI component. Enables out-of-bounds writes, potentially allowing host code execution.

• CVE-2025-41238 - Heap overflow in the PVSCSI controller. Could be exploited for host code execution in specific configurations.

• CVE-2025-41239 - Uninitialized memory usage in the vSockets component. Leads to information disclosure through memory leaks.

Impact

- Remote Code Execution
- Privilege Escalation
- Information Disclosure

Solution/ Workarounds

Before installation of the software, please visit the vendor web-site for more details.

Apply fixes issued by VMware:

- VMware Workstation: Update to 17.6.4
- VMware Fusion: Update to 13.6.4
- VMware ESXi: Update to ESXi80U2e-24789317 or ESXi70U3w-24784741
- VMware Tools: Update to 13.0.1.0

Reference

- https://cybersecuritynews.com/vmware-esxi-and-workstation-vulnerabilities/
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35877

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.