CERT-EU

Security Advisory 2025-026

Critical Vulnerabilities in VMWare Products

2025-07-18 — v1.0

TLP:CLEAR

History:

- *18/07/2025 — v1.0 – Initial publication*

Summary

On July 15, 2025, VMware released a security advisory addressing 3 critical vulnerabilities in its products that would allow an attacker to execute code on vulnerable devices [1].

It is recommended updating affected products as soon as possible, prioritising the ones hosting virtual machines that are Internet facing.

Note: These vulnerabilities were exploited as zero-days during the Pwn2Own Berlin 2025 hacking contest in May 2025.

Technical Details

The vulnerability **CVE-2025-41236**, with a CVSS score of 9.3, is an integer-overflow in the VMXNET3 virtual network adapter. A malicious actor with local administrative privileges on a virtual machine with VMXNET3 virtual network adapter may exploit this issue to execute code on the host. Non VMXNET3 virtual adapters are not affected by this issue.

The vulnerability **CVE-2025-41237**, with a CVSS score of 9.3, is an integer-underflow in VMCI (Virtual Machine Communication Interface) that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox whereas, on Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.

The vulnerability **CVE-2025-41238**, with a CVSS score of 9.3, is a heap-overflow vulnerability in the PVSCSI (Paravirtualized SCSI) controller that leads to an out of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host. On ESXi, the exploitation is contained within the VMX sandbox and exploitable only with configurations that are unsupported. On Workstation and Fusion, this may lead to code execution on the machine where Workstation or Fusion is installed.

Affected Products

The following products are affected by at least one of the vulnerabilities:

- VMware Cloud Foundation (ESX component)
- VMware vSphere Foundation (ESX component)
- VMware ESXi
- VMware Workstation
- VMware Fusion
- VMware Telco Cloud Platform
- VMware Telco Cloud Infrastructure
- VMware Tools

For a detailed list of the versions, please refer to the vendor's advisory [1].

Recommendations

It is recommended updating affected products as soon as possible, prioritising the ones hosting virtual machines that are Internet facing.

References

[1] https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/35877