مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerabilities in VMware Products

Tracking #:432317493

Date:17-07-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Broadcom issued a critical advisory addressing four newly discovered vulnerabilities in VMware ESXi, Workstation, Fusion, Tools, and multiple cloud platforms.

TECHNICAL DETAILS:

Broadcom issued a critical advisory (VMSA-2025-0013) addressing four newly discovered vulnerabilities (CVE-2025-41236 through CVE-2025-41239) in VMware ESXi, Workstation, Fusion, Tools, and multiple cloud platforms.
Three of the four CVEs have CVSSv3 scores of 9.3, signifying critical severity, and enable privilege escalation or arbitrary code execution from within a guest VM to the host machine.
There are no available workarounds, making patch deployment essential. Affected products include VMware ESXi 7/8, VMware Workstation 17, Fusion 13, Cloud Foundation, and Telco Cloud Platform.
Vulnerabilities are exploitable by attackers with local administrative access to virtual machines.

Vulnerability Details

1. **CVE-2025-41236 – VMXNET3 Integer Overflow**
   - Severity: Critical (CVSS 9.3)
   - Affected Component: VMXNET3 network adapter
   - Impact: Arbitrary code execution on host from VM
   - Condition: Exploitable via guest VM with VMXNET3
   - Status: Patched in ESXi 8.0, 7.0, Workstation 17.6.4, Fusion 13.6.4

2. **CVE-2025-41237 – VMCI Integer Underflow**
   - Severity: Critical (CVSS 9.3)
   - Affected Component: Virtual Machine Communication Interface (VMCI)
   - Impact: Out-of-bounds write leading to host compromise
   - Notes: Sandbox-escaped in Workstation/Fusion
   - Status: Patched across all platforms

3. **CVE-2025-41238 – PVSCSI Heap Overflow**
   - Severity: Critical (CVSS 9.3)
   - Affected Component: PVSCSI controller
   - Impact: Code execution in VMX process on host
   - Notes: Exploitable only in unsupported VM configurations on ESXi
   - Status: Patch available, update required

4. **CVE-2025-41239 – vSockets Memory Leak**
   - Severity: Important (CVSS 7.1)
   - Affected Component: vSockets
   - Impact: Information disclosure through uninitialized memory
   - Platforms: Affects VMware Tools on Windows, ESXi, Workstation, Fusion
   - Status: Resolved in VMware Tools 13.0.1.0, 12.5.3

Fixed versions:

- **ESXi 8.0** → Update to ESXi80U3f-24784735 or ESXi80U2e-24789317
- **ESXi 7.0** → Update to ESXi70U3w-24784741
- **Workstation 17.x** → Update to 17.6.4
- **Fusion 13.x** → Update to 13.6.4
- **VMware Tools** (Windows) → Update to 13.0.1.0 or 12.5.3 for 32-bit
- **Cloud Foundation** → Apply **async patching** (see KB88287)

RECOMMENDATIONS:

- Patch Immediately: Apply the fixed versions for each product as listed in the advisory's Response Matrix.
- Restrict Guest VM Admin Access: Only allow administrative privileges to trusted VM users; these flaws require local admin access to exploit.
- Test in Staging Environments: Before production deployment, validate patch compatibility and VM behavior in a controlled test environment.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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