NCA-11.032525 – NCERT Advisory – VMware Virtualization Vulnerabilities Leading to Ransomware Deployment

Introduction

A critical security threat has emerged due to multiple vulnerabilities in VMware virtualization products, tracked as CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226. These vulnerabilities allow attackers to bypass security controls, escape virtual machine (VM) containment, and deploy ransomware at scale. Exploitation of these flaws has been observed in active attacks, compromising enterprise infrastructure and leading to severe operational disruptions. Organizations relying on VMware ESXi, Workstation, and Fusion must act swiftly to mitigate risks and secure their environments.

Impact

Exploitation of these vulnerabilities can result in:

1. **VM Escape & Hypervisor Compromise**: Attackers can execute code outside the VM boundary, gaining control over the hypervisor.
2. **Privilege Escalation**: Kernel-level access on ESXi hosts can be obtained, allowing full administrative control.
3. **Credential Theft & Lateral Movement**: Attackers can extract authentication data from hypervisor memory to access vCenter and other critical systems.
4. **Ransomware Deployment**: Entire VM clusters, including business-critical applications, can be encrypted and rendered inoperable.
5. **Backup Deletion & Data Exfiltration**: Attackers can delete snapshots and backups stored in vSphere datastores, enforcing ransom demands through double extortion tactics.

Vulnerability Details

The attack chain exploits three VMware vulnerabilities in sequence:

- **CVE-2025-22224 (CVSS 9.3)**: A heap overflow in VMware's VMCI driver allows attackers with VM administrator privileges to execute code on the host's VMX process, breaching the hypervisor layer.
- **CVE-2025-22225 (CVSS 8.2)**: An arbitrary write vulnerability that enables privilege escalation, granting kernel-level control over ESXi hosts.
- **CVE-2025-22226 (CVSS 7.1)**: A hypervisor memory leak flaw that exposes credentials, allowing attackers to pivot to vCenter and other enterprise systems.

Threat actors gain initial access via internet-facing VMs, leveraging web shells or stolen credentials. Once inside, they exploit CVE-2025-22224 for VM escape, CVE-2025-22225

for privilege escalation, and CVE-2025-22226 to steal credentials. The attack culminates in full system compromise, ransomware deployment, and data exfiltration.

Security researchers have observed more than 41,500 exposed VMware ESXi hypervisors vulnerable to CVE-2025-22224 as of March 4, 2025. Sectors such as healthcare and finance report the highest attack rates, with ransomware encrypting entire patient record systems and transaction databases within 47 minutes of initial access.

Affected Systems

The following VMware products are vulnerable:

- **VMware ESXi**: Versions prior to ESXi80U3d-24585383, ESXi80U2d-24585300, ESXi70U3s-24585291, ESXi670-202503001
- **VMware Workstation**: Versions prior to 17.6.3
- **VMware Fusion**: Versions prior to 13.6.3
- **VMware Cloud Foundation & Telco Cloud Platform**: Require specific asynchronous patches

Recommendations & Action Items

1. **Immediate Mitigation Measures**
    - Restrict external access to VMware management interfaces using firewall rules.
    - Implement micro-segmentation to isolate ESXi, vCenter, and critical infrastructure.
    - Enable logging and actively monitor ESXi logs (/var/log/hostd.log) for anomalies.
    - Review privileged account access and enforce multi-factor authentication (MFA).
2. **Patching and Updates**
    - Apply the following patched versions immediately:
        - VMware ESXi 8.0: **ESXi80U3d-24585383, ESXi80U2d-24585300**
        - VMware ESXi 7.0: **ESXi70U3s-24585291**
        - VMware ESXi 6.7: **ESXi670-202503001**
        - VMware Workstation 17.x: **17.6.3**
        - VMware Fusion 13.x: **13.6.3**
    - Ensure updates are downloaded only from official VMware sources.

PKCERT

3. **Hardening Security Configurations**
    - Disable unnecessary services and enforce the principle of least privilege.
    - Implement network segmentation to prevent lateral movement.
    - Deploy endpoint detection and response (EDR) solutions to identify threats.
4. **Incident Response and Recovery**
    - Conduct forensic analysis if suspicious activity is detected.
    - Restore affected VMs from clean, offline backups.
    - Increase security monitoring for known indicators of compromise (IoCs).

References

1. **VMware Security Advisories**: https://www.vmware.com/security/advisories.html
2. **Sygnia Report:** https://www.sygnia.com/research/vmware-ransomware-attacks
3. **Shadowserver Vulnerability Scan**: https://www.shadowserver.org/reports/vmware-exploited
4. **CISA KEV List**: https://www.cisa.gov/known-exploited-vulnerabilities

Call to Action

National CERT urges all organizations using VMware products to apply patches immediately. Given the active exploitation and severity of these vulnerabilities, prompt remediation is essential to prevent ransomware deployment and infrastructure compromise.

PKCERT