CVE-2025-22224, CVE-2025-22225 and CVE-2025-22226: Multiple severe Vulnerabilities in VMware

Vairav CVE Report

Date: 2025-03-05

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

Multiple vulnerabilities—**CVE-2025-22224, CVE-2025-22225, and CVE-2025-22226**—have been identified in VMware products, including ESXi, Workstation, and Fusion. The most severe, CVE-2025-22224, allows for code execution with a **CVSS score of 9.3**. Exploitation of these vulnerabilities could lead to system compromise and information disclosure.

VULNERABILITY DETAILS

CVE-2025-22224

- **Description:** A Time-of-Check Time-of-Use (TOCTOU) vulnerability leading to an out-of-bounds write. An attacker with local administrative privileges on a virtual machine could exploit this to execute code as the VMX process on the host.
- **Impact:** Potential for attackers to execute arbitrary code on the host system, leading to full system compromise.
- **CVSS Score:** 9.3 (Critical)

CVE-2025-22225

- **Description:** An arbitrary write vulnerability where an attacker with privileges within the VMX process could escape the sandbox environment.
- **Impact:** Allows attackers to execute code outside the virtual machine, potentially compromising the host system.
- **CVSS Score:** 8.2 (High)

CVE-2025-22226

- **Description:** An out-of-bounds read in the Host Guest File System (HGFS) that could leak memory from the VMX process.
- **Impact:** Attackers could access sensitive information from the host system's memory.
- **CVSS Score:** 7.1 (High)

AFFECTED VERSIONS

- **VMware ESXi:** Versions 7.0 and 8.0
- **VMware Workstation:** Version 17.x
- **VMware Fusion:** Version 13.x
- **VMware Cloud Foundation:** Versions 4.x and 5.x
- **VMware Telco Cloud Platform:** Versions 2.x, 3.x, 4.x, and 5.x
- **VMware Telco Cloud Infrastructure**: Versions 2.x and 3.x

EXPLOIT DETAILS

These vulnerabilities have been exploited in the wild, particularly affecting environments where VMware products are used for virtualization. Attackers with administrative access to a virtual machine can exploit these flaws to execute code on the host system, escape the sandbox and leak memory ultimately leading to potential system compromise and data breaches.

RECOMMENDED ACTIONS

Patch & Upgrade:

Upgrade to the latest VMware versions:

- **VMware ESXi 8.0:** Update to ESXi80U3d-24585383 or ESXi80U2d-24585300
- **VMware ESXi 7.0:** Update to ESXi70U3s-24585291
- **VMware Workstation 17.x:** Update to version 17.6.3
- **VMware Fusion 13.x:** Update to version 13.6.3
- **VMware Cloud Foundation 5.x:** Apply async patch to ESXi80U3d-24585383
- **VMware Cloud Foundation 4.x:** Apply async patch to ESXi70U3s-24585291
- **VMware Telco Cloud Platform 5.x, 4.x, 3.x, 2.x**: Update to ESXi 7.0U3s, ESXi 8.0U2d, and ESXi 8.0U3d.
- **VMware Telco Cloud Infrastructure 3.x, 2.x:** Update to ESXi 7.0U3s.

ADDITIONAL SECURITY MEASURES

- **Restrict Administrative Access:** Limit administrative privileges on virtual machines to trusted users only.
- **Network Segmentation:** Isolate critical systems and services to minimize potential attack vectors.
- **Regular Monitoring**: Implement continuous monitoring to detect and respond to unauthorized activities promptly.

REFERENCES

- https://thehackernews.com/2025/03/vmware-security-flaws-exploited-in.html
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390
- https://app.opencve.io/cve/CVE-2025-22224
- https://app.opencve.io/cve/CVE-2025-22225
- https://app.opencve.io/cve/CVE-2025-22226

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com