Security Advisory 2025-005

Several Vulnerabilities in VMware Products

2025-03-05 — v1.0

TLP:CLEAR

History:

- *05/03/2025 — v1.0 – Initial publication*

Summary

On March 4, 2025, Broadcom issued an advisory regarding multiple vulnerabilities in VMware products. An attacker with access to a virtual machine could escape it to execute code on the host. Those vulnerabilities are being exploited in the wild [1].

It is recommended applying update as soon as possible.

Technical Details

The vulnerability `CVE-2025-22224`, with a CVSS score of 9.3, is a TOCTOU (Time-of-Check Time-of-Use) vulnerability 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.

The vulnerability `CVE-2025-22225`, with a CVSS score of 8.2, is an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox.

The vulnerability `CVE-2025-22226`, with a CVSS score of 7.1, is an information disclosure vulnerability due to an out-of-bounds read in the Host Guest File System (HGFS). A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process.

Products Affected

Those vulnerabilities effect : - VMware ESXi 7.0, 8.0 - VMware Workstation 17.x - VMware Fusion 13.x - VMware Cloud Foundation 4.5.x, 5.x - VMware Telco Cloud Platform 5.x, 4.x, 3.x, 2.x - VMware Telco Cloud Infrastructure 3.x, 2.x

Recommendations

CERT-EU recommends updating to the latest version of the affected product as soon as possible to mitigate those vulnerabilities [1].

References

[1] https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390