NATIONAL CSIRT-CY

CVE-2025-22224 **06/03/2025**

VMware ESXi, Workstation and Fusion vulnerabilities

Executive Summary

Three actively exploited vulnerabilities in VMware ESXi, Workstation and Fusion products are being addressed in the latest security updates from Broadcom.

- CVE-2025-22224 (CVSS score: 9.3) - A Time-of-Check Time-of-Use (TOCTOU) vulnerability that enables an out-of-bounds write. With local admin rights a malicious actor on a VM could exploit this in order to execute code as the virtual machine's VMX process running on the host
- CVE-2025-22225 (CVSS score: 8.2) - An arbitrary write vulnerability that a can be exploited by a malicious actor with admin privileges within the VMX process potentially leading to a sandbox escape
- CVE-2025-22226 (CVSS score: 7.1) - An information disclosure vulnerability caused by an out-of-bounds read in HGFS, which a malicious actor with administrative privileges in a VM may be able to exploit in order to leak memory from the VMX process

We urge users of the aforementioned VMware products to update to the latest version:
https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25390

Common Weakness Enumeration

https://cwe.mitre.org/data/definitions/367.html

Common Vulnerabilities & Exposures

https://nvd.nist.gov/vuln/detail/CVE-2025-22224

Affected Systems

Product Version
VMware ESXi 8.0 ESXi80U3d-24585383
VMware ESXi 8.0 ESXi80U2d-24585300
VMware ESXi 7.0 ESXi70U3s-24585291
VMware Workstation 17.6.3
VMware Fusion 13.6.3
VMware Cloud Foundation 5.x, 4.5.x
Telco Cloud Platform 5.x, 4.x, 3.x

Please distribute this information among your subsidiaries and partners, and also share with us any pertinent information and findings you may have (e.g IOCs, TTPs etc)

The Digital Security Authority extends its appreciation for the continued collaboration.

Disclaimer

Organizations are advised to consult with relevant cybersecurity professionals and follow best practices for their specific environments.