Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 264 **20-5-2024**

Name: Multiple VMware Workstation and Fusion Zero-Day Vulnerabilities Exploit in the Wild

Threat Classification: Vulnerability

Affected Software / Area:

- VMware Workstation 17.5.1, VMware Fusion 13.5.1

Summary:

Multiple zero-day vulnerabilities have been discovered in VMware Workstation and Fusion software, potentially exposing users to severe security risks. The vulnerabilities, identified as **CVE-2024-22267**, **CVE-2024-22268**, and **CVE-2024-22269**, can allow attackers to execute arbitrary code, trigger buffer overflows, and obtain sensitive information. Exploitation of these vulnerabilities could lead to code execution, denial of service, and information disclosure.

Severity	**High**
Attack Vector	**Buffer Overflow**

Recommendations:

- It is recommended that Immediately upgrade to the latest versions of VMware Workstation and Fusion, which contain patches for these vulnerabilities.

- VMware has issued the updated release of VMware Workstation 17.5.2 Pro version link (https://docs.vmware.com/en/VMware-Workstation-Pro/17.5.2/rn/vmware-workstation-1752-pro-release-notes/index.html#Resolved%20Issues-Security%20Issues)
- Avoid opening suspicious or unknown virtual machines or files, as they may be crafted to exploit these vulnerabilities.
- Organizations should test their assets for the identified vulnerabilities and apply security patches or mitigation steps immediately.
- Implement robust monitoring solutions to detect any unusual activity or attempts to exploit these vulnerabilities.
- Establish a proactive patch management process to ensure timely deployment of security updates for all software and systems.
- Educate users about the risks associated with zero-day vulnerabilities and the importance of keeping software up-to-date.
- In case of any incident, please report to this office, through PTA CERT Portal and email.