PTA Cyber Security Advisory No: 071

18-March-2020

Name: VMware products Privilege Escalation and Use-after-free Vulnerability (CVE-2020-3947 and CVE-2020-3948)

Threat Classification: Privilege Escalation & Code Execution

Affected Systems: Affects the following vmware products:

i. VMware Workstation Pro / Player
ii. VMware Fusion Pro / Fusion
iii. VMware Horizon Client for Windows
iv. VMware Remote Console for Windows

Summary:

VMware Workstation and Fusion have use-after or use-after-free vulnerability which may lead to code execution on the host from the guest or may allow the attackers to create a denial-of-service condition of the vmnetdhcp service running on the host machine. Linux guest VMs, running on same VMware products also have a privilege escalation vulnerability due to improper file permissions in Cortado Thinprint. Local attackers with non-administrative access to Linux guest VM with virtual printing enabled may exploit this issue to elevate their privileges to root on the same guest VM.

Attack Severity	Critical
Attack Type	Privilege Escalation & Remote Code Execution
Workarounds	None

© Copyright 2019-2020, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, modification of this document is strictly prohibited.

For further details, please visit following vendor official link:

https://www.vmware.com/security/advisories/VMSA-2020-0004.html

Recommendations:

- Please visit the resolution matrix present at the following official website link for the remediation of the aforementioned vulnerabilities:
    - https://www.vmware.com/security/advisories/VMSA-2020-0004.html
- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.
- In all cases, also ensure that devices to be upgraded to new release meet the requirements set by the vendor.
- Whenever required, access the system with minimal access rights and privileges.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoid download/use of cracked and pirated software.
- Designate a PoC from your security / Network team (if yet not designated), for seeking assistance and reporting security issues.
- In case of any incident, please report to this office.

© Copyright 2019-2020, Pakistan Telecommunication Authority. All Rights Reserved.
Unauthorized use, modification of this document is strictly prohibited.