



Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 116

27-11-2020

Name: VMware products Use-after-free and Privilege Escalation vulnerabilities (CVE-2020-4004, CVE-2020-4005)

Threat Classification: Code Execution and Privilege Escalation

Affected Systems: Affects the following VMware products:

- VMware ESXi
- VMware Workstation Pro / Player
- VMware Fusion Pro / Fusion
- VMware Cloud Foundation

Summary:

Use-after-free and privilege escalation critical vulnerabilities exist in the above mentioned vmware products, which may allow an attacker to execute code or escalate privileges (in a way certain system calls are being managed) on the affected system.

Severity	CRITICAL
Attack Vector	Local
Privileges required	Low

For further details, please visit following official link:

<https://www.vmware.com/security/advisories/VMSA-2020-0026.html>

Recommendations:

- Please visit the 'Fixed Version' column of the 'Response Matrix' present at the following official website link for the remediation of the aforementioned vulnerabilities:
<https://www.vmware.com/security/advisories/VMSA-2020-0026.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.