Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 129   08-03-2021

Name: Vmware products Remote Code Execution Vulnerability (CVE-2021-21972, CVE-2021-21973, CVE-2021-21974)

Threat Classification: Remote code execution

Affected Systems: Affects the following VMware products:

- VMware ESXi

- VMware vCenter Server (vCenter Server)

- VMware Cloud Foundation (Cloud Foundation)

Summary:

Multiple vulnerabilities in VMware ESXi and vSphere Client (HTML5) were privately reported to VMware. A malicious actor with network access may exploit these issues to take control of an affected system.

Severity	CRITICAL
Attack Vector	Network
Privileges required	None

For further details, please visit following official link:
https://www.vmware.com/security/advisories/VMSA-2021-0002.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-2021-0002.html

- In all cases, ensure the availability of stable version, before upgrade, by the relevant vendor.

- 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.