Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No:080 **04-May-2020**

Name: VMware ESXi Stored Cross-Site Scripting (XSS) Vulnerability (CVE-2020-3955)

Threat Classification: Cross-Site Scripting (XSS)

Affected Systems: Affects the following VMware product:

- VMware ESXi

Summary:

VMware ESXi Host Client does not properly neutralize script-related HTML when viewing the attributes of virtual machines. A malicious actor with access to modify system properties of a virtual machine from inside the guest OS may be able to inject malicious script which will be executed by victim's browser when viewing this virtual machine via the Host Client.

Severity	HIGH
Attack Vector	Network
Privileges required	None

For further details, please visit following official link:
https://www.vmware.com/security/advisories/VMSA-2020-0008.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 vulnerability:
  https://www.vmware.com/security/advisories/VMSA-2020-0008.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.