



Pakistan Telecom Authority Headquarter, Islamabad

PTA Cyber Security Advisory No: 077

27-April-2020

Name: VMware vCenter Server Sensitive information disclosure vulnerability in the VMware Directory Service (vmdir) (CVE-2020-3952)

Threat Classification: Information Disclosure vulnerability

Affected Systems: Affects the following VMware product:

- VMware vCenter Server

Summary:

Under certain conditions, vmdir as part of an embedded or external Platform Services Controller (PSC), does not correctly implement the access controls. A malicious actor with network access to port 389 on an affected vmdir deployment may be able to get highly sensitive information such as administrative account credentials which could be used to compromise vCenter Server or other vmdir dependent services for authentication.

Attack Severity	Critical
Attack Vector	Network
Privileges Required	None

For further details, please visit following vendor official link:

<https://www.vmware.com/security/advisories/VMSA-2020-0006.html>

Recommendations:

- Please visit the 'Response Matrix' present at the following official website link for the remediation of the aforementioned vulnerability:
 - <https://www.vmware.com/security/advisories/VMSA-2020-0006.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.