Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:124 13-01-2021

Name: Microsoft Defender antivirus zero-day exploit patched (CVE-2021-1647)

Summary:

Microsoft has addressed a zero-day remote code execution vulnerability found in the Malware Protection Engine component (mpengine.dll) of Microsoft Defender antivirus, which has been reported to be exploited by threat actors before the patch was released.

Attack Severity	**Critical**
Attack Type	Remote Code Execution
Privileges Required	Low

For further details, please visit following link:
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1647

Recommendations:

- It is highly recommended to update the Microsoft Defender Malware Protection Engine at earliest for the remediation of the aforementioned vulnerability.
- Update all software including Operating Systems, Servers, etc. to the latest and stable versions with appropriate patches.
- Install, regularly maintain and update Anti-Malware solution from a well reputed vendor.

- System Administrators/ Network Administrators to configure host-based firewalls to block outbound connections from Excel.exe, Winword.exe, Wordpad.exe, Mshta.exe, Noptepad.exe, Eqnedt32.exe and ctfmon.exe as Anti-malware solutions alone cannot fully protect against APT attacks.
- Execution of unsigned executables from sensitive webservers and endpoints must be blocked.
- Regularly provide Cyber security awareness sessions for employees and continuously arrange capacity building of the relevant technical resources.
- Do not download attachments from emails unless they are from the trusted source.
- Avoid download/use of cracked and pirated software.
- In case of any incident, please report to this office.