Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 143 **13-09-2021**

Name: Microsoft MSHTML Remote Code Execution Vulnerability

(CVE-2021-40444)

Threat Classification: Remote code execution

Summary:

Vulnerability is found in Microsoft MSHTML which causes the attempt to exploit by using specially-crafted Microsoft Office documents. An attacker could craft a malicious ActiveX control to be used by a Microsoft Office document that hosts the browser rendering engine. The attacker would then have to convince the user to open the malicious document. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

Severity	**Critical**
Attack Vector	Network
Privileges required	None

For further details, please visit following link:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444

Recommendations:

- Please visit the website link and check mitigations and workaround of the aforementioned vulnerabilities:

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444

- Microsoft Defender Antivirus and Microsoft Defender for Endpoint both provide detection and protections for the known vulnerability. Customers should keep antimalware products up to date and the users who utilize automatic updates do not need to take additional action.
- Enterprise customers who manage updates should select the detection **build 1.349.22.0** or **newer** and deploy it across their environments.
- Disabling the installation of all ActiveX controls in Internet Explorer mitigates this attack. This can be accomplished for all sites by configuring the Group Policy using your Local Group Policy Editor **or** by updating the registry.
- 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.