Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No: 151 **01-06-2022**

NAME: Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability **(CVE-2022-30190)**

Threat Classification: Remote Code Execution.

Affected Versions:

Microsoft Office versions Office 2013, Office 2016, Office 2019, and Office 2021, as well as Professional Plus editions, are impacted

Summary:

A remote code execution vulnerability exists when MSDT is called using the URL protocol from a calling application such as Word. An attacker who successfully exploits this vulnerability can run arbitrary code with the privileges of the calling application. The attacker can then install programs, view, change, delete data, or create new accounts in the context allowed by the user's rights.

Microsoft issues workaround sections for important information about steps to protect the system from this vulnerability from the following link of Microsoft's official website mentioned:

https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

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

Recommendations:

- Please visit the website link and check **workarounds** for the aforementioned vulnerabilities: https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

- It is recommended to update the security by checking the latest Security Updates in MS Widows Security and Update table.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- 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.