Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No.:092 **23-July-2020**

Threat Classification: Remote Code Execution

Name: Microsoft Windows DNS Server Critical Wormable RCE Vulnerability (CVE-2020-1350)

Affected Systems: Affects the following Microsoft products:

- Windows Server 2008, 2012, 2016, 2019

Summary:

This vulnerability exists in Windows Domain Name System servers when they fail to properly handle the requests. Windows servers that are configured as DNS servers are at risk due to this vulnerability that allows an attacker to run arbitrary code. To exploit the vulnerability, an attacker could send malicious requests to a Windows DNS server.

Attack Severity	CRITICAL
Attack Vector	Network
Attack Type	Code Execution
Privileges Required	None

For further details, please visit following official website link:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

For Security update guidance and release notes, please visit following link:
https://portal.msrc.microsoft.com/en-us/security-guidance

Recommendations:

- Please visit ‘Security Updates’ section of the following official website link for the security updates of the aforementioned vulnerability:
  https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350

- It is strongly recommended to patch this critical vulnerability as soon as possible.

- 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, run software 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.

- In case of any incident, please report to this office.