CRITICAL ADVISORY

Cyber Peace Foundation

OVERVIEW

BLUE KEEP (CVE-2019-0708) is a critical remote code execution vulnerability in Remote Desktop Protocol Service. This vulnerability is pre-authentication and does not require any user interaction to spread. It spreads rapidly in a worm-like fashion thus making it extremely critical. Worldwide millions of users use RDP service for remote controlled administration.

On May 14, Microsoft released a patch for critical vulnerability.

AFFECTED PLATFORMS

It exists within the RDP used by Mircosoft Windows OS such as Windows 7, Windows 2008 R2, Windows Server 2008, Windows XP, and Windows Server 2003. An attacker can send specially crafted code to any of the above mentioned Operating systems, if RDP is enabled.

DESCRIPTION

RDP uses TCP port 3389 by default to interact remotely. It enables connections between clients and servers by defining the data communicated between them in virtual channels.

Virtual Channels are bidirectional data pipelines which enables transfer of data between any two systems. It can be of two types:

- Static Virtual Channel- The ones already existing in your system.
- Dynamic virtual channels- It extends the existing SVC for Remote Desktop Services by binding SVM Channel names to numbers within the driver TermDD.sys.

Windows uses different names to represent each channel and each channel has specific function. RDP internally creates MS_T120 channel by default when a connection is established. IT does not expect clients to create another channel with the same name over a network.

RDP reserves channel 31 in slot 0x1F with the name MS_T120 by default, but does not authenticate other channels of similar names. This, makes the system vulnerable.

An attacker, exploits this vulnerability by creating a channel by the name of MS_T120 and allotting it a different number. This results in the current RDP session having the same channel in two different places within the available channels.

For example, say a malicious channel MS_T120 exists on channel number 25 and the default MS_T120 is on channel number 31.

Here, when an attacker sends data through the malicious channel, the driver TermDD.sys attempts to respond by sending an error message and clearing the pointer at the user controlled slot. But, the default MS_T120 pointer in slot 0x1F isn't cleared. Thus, a dangling pointer remains tied to channel number 31, leading to use-after-free vulnerability. Thus, enabling the attacker to open a MS_T120 channel through channel number 25 (the user controlled slot) and send malicious code. After successfully sending the packets, the attacker will have the ability to add accounts with full user rights; view, change, or delete data, or install new programs. Making the system vulnerable by giving the attacker kernel-level privileges.

CAUTION: This vulnerability is pre-authentication and requires no user interaction.

HOW TO PREVENT

1. Patch your system with the latest Microsoft update as soon as possible.

2. Enabling Network Level Authentication forces a session to be authenticated and monitors incoming RDP sessions for any attempt to write a custom channel with the name of MS_T120 from unauthorized users.

3. Block TCP Port 3389 at enterprise perimeter firewall, as it prevents attacker from exploiting BlueKeep from outside user network. However, doing so has little effect on preventing unauthenticated sessions from being initiated inside a network.

4. Disable unnecessary services which are not used by OS to limit vulnerability.