https://doi.org/10.46335/IJIES.2022.7.6.9 **e-ISSN: 2456-3463**
Vol. 7, No. 6, 2022, PP. 37-39

International Journal of Innovations in Engineering and Science, www.ijies.net

Review on Blue Keep Vulnerability

Dr. Snehal Golait [1] ,Vaibhav Malgewar [2] ,Hrishikesh Somchatwar [3], Pranay Kotangale [4] ,Ritik Kuthe [5] , Nitin Kumar [6]

[1]Assitant Professor, [2,3,4,5,6] Students

Department of Computer Science, Priyadarshini College of Engineering,Nagpur, India

snehal.golait@gmail.com

***Received on**: 20 May ,2022* ***Revised on**: 20 June ,2022,* ***Published on**: 22 June,2022*

***Abstract –** This paper gives a short review on BlueKeep Vulnerablity . BlueKeep is a significant risk for Remote Coding in Microsoft's RDP service. Since being at risk is dangerous, it has attracted a lot of attention from the security community, which is in the same category as EternalBlue MS17-010 and Conficker MS08-067. We have published an in-depth analysis of BlueKeep vulnerability to help you get the full picture. In this paper we will demonstrate a new approach to use Bluekeep vulnerability. A few days ago, a Metasploit provider - zerosum0x0 - applied for a draw from a framework containing the BlueKeep exploitation module (CVE-2019-0708). The Rapid7 team also published an article about this abuse on their blog.To date, the module has not been integrated with the main Metasploit branch (still a download application) and only manages Windows 2008 R2 and Windows 7 SP1, 64-bit versions. In addition, the module is now calculated as a Manual as the user needs to provide additional information about the target, otherwise, it may be in danger of crashing through the BSOD.*

I - INTRODUCTION

Since the launch of the IT Industry a lot of work has been done in the Operating System, there are 50+ types of Applications available online yet at the same time that it is possible and obvious that we are including the Windows App in this project we will explain. show a live Short of How the World and One of the Most Risky Ransomware Attacks In 2017, The Attack was tested to affect more than 200,000 PCs in 150 countries. WannaCry Attack Known for Hacking Conditions The Easy Way to Control Computers, Windows-7 is the most common OS in the world and has a major problem that creates the unfortunate Few Data in Asia / World name the vulnerability that causes this attack is as follows. BlueKeep (CVE-2019-0708) is a security risk derived from the use of Microsoft Remote Desktop Protocol (RDP), which allows for the possibility of remote control code.

1. BlueKeep

BlueKeep exploits have the ability to spread in a worm-like manner and replicate without the need for user interaction. According to Microsoft, the attacker may be able to send malware packages specially designed for uninstalled Windows operating systems with RDP enabled. After successfully sending packets, the attacker will be able to perform a number of actions, including adding new user accounts, installing malicious programs and making changes to the data.

BlueKeep proof of concept (PoC) takes advantage of denial-of-service (DoS) attacks and remote coding (RCE) in vulnerable systems demonstrated by researchers from Twitter, McAfee, Zerodium and Kaspersky. As of this writing, BlueKeep attacks have never been seen in the wild, but Proofpoint security researchers have reported low-level scanning activity looking for compromised systems.

BlueKeep code modification was released on May 14, 2019 for all supported Windows operating systems, as well as Windows XP and Server 2003. In addition to updating and updating Windows operating systems to prevent BlueKeep exploitation, network administrators should also consider :

- Disable unused and unnecessary RDP resources.
- Blocks TCP Port 3389.
- Enable network level verification for RDP services to prevent attackers from creating remote control code without authorized data.

II- FACTUAL DESCRIPTION

Blue Keep is a basic weakness of Remote Code Generating in Microsoft RDP management. Since vulnerabilities can create worms, much attention has been given to local safety, being in the same category as Eternal Blue MS17-010 and Conifer MS08-067. We have expanded the internal and external investigation of Blue Keep weaknesses to help you get the full picture. This unfortunate Big Attack is another Method called payload / Virus however it may change or Work in all Operating Systems except Linux based OS.

Prerequisites

For this scenario to work, we used the following:

- VirtualBox 6 for hosting the target Windows VM
- An outdated Windows 2008 R2 64bit .iso image; the latest Hotfixes installed on our target VM were: KB2888049 and KB976902
- A Linux machine where to setup Metasploit (it can be virtual machine or physical)

III- SETTING UP THE TARGET MACHINE

The target VM had the following properties:

- 2GB RAM
- 1 Core processor
- 30 GB HDD storage size

IV-RUNNING THE BLUEKEEP EXPLOIT MODULE

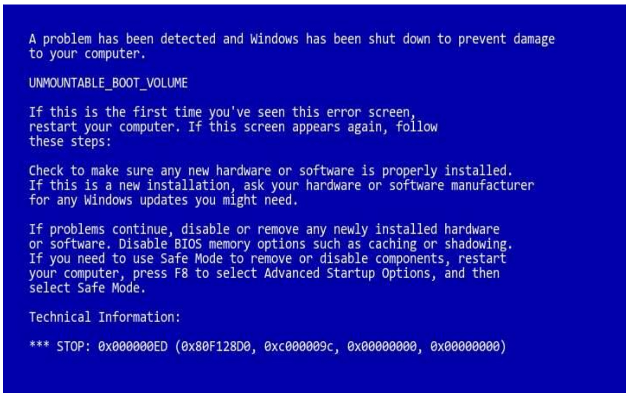
The first thing is to change the parameter GROOMSIZE to 50. This is related to the amount of memory the virtual machine has and this is the value that worked for our situation.

- Download VM
- Install windows 7 or windows server 2012 or later version.
- Connect with bridge adapter in NAT.
- Both machines must be in network.
- Open Linux Attacker machine.
- Use msfconsole/Metasploit.
- Search for the module eternal blue/bluekeep/double pulsar.
- Enter the IP and port of the target machine.
- Turn on force exploit = True (fdisable=0).
- Run exploit.

V- CONCLUSIONS

Although the proposed BlueKeep Metasploit module does not provide you with a remote shell with automatic configuration, its addition to Metasploit prompts system administrators and home users to attach their Windows devices. We are confident that the security community will soon find a way to automatically find the first NPP address, which will make this exploitation fully credible for many purposes.

Fig 1- Image Source -Self



```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.

UNMOUNTABLE_BOOT_VOLUME

If this is the first time you've seen this error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical Information:

*** STOP: 0x000000ED (0x80F128D0, 0xc000009c, 0x00000000, 0x00000000)
```

Fig 2- Image Source -Self

REFERENCES

[1] *Y. Kraev, G. Firsov and D. Kandakov, "Authentication via RDP Using Electronic Identifiers," 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), 2021, pp. 2361-2365, doi: 10.1109/ElConRus51938.2021.9396471.*

[2] *Y. Fadlallah, M. Sbeiti, M. Hammoud, M. Nehme and A. Fadlallah, "On the Cyber Security of Lebanon: A Large Scale Empirical Study of Critical Vulnerabilities," 2020 8th International Symposium on Digital Forensics and Security (ISDFS), 2020, pp. 1-6, doi: 10.1109/ISDFS49300.2020.9116446.*

[3] *O. Valea and C. Oprişa, "Towards Pentesting Automation Using the Metasploit Framework," 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP), 2020, pp. 171-178, doi: 10.1109/ICCP51029.2020.9266234.*