SMBGHOST

Project Vulnerability Description Report

Zaina Shahid

TABLE OF CONTENTS

OVERVIEW OF THE REPORT:

This report provides a comprehensive description of the SMBGhost vulnerability, also known as CVE-2020-0796, affecting systems that utilize the Server Message Block (SMB) protocol, specifically SMBv3. This is a critical vulnerability for affected systems as it allows remote code execution, which could potentially grant hackers to have complete control over the system thereby leading to data breach, server infiltration and network sabotage.

The report provides an overview of the technical aspects of this vulnerability such as its description and the versions of Windows affected by it. SMBGhost results from mishandling compressed packets of information within the SMBv3 protocol that can be exploited to execute any arbitrary code on the target computer.

The report emphasizes just how critical this bug is because it requires no authentication to exploit and may become wormable implying it spreads automatically between vulnerable computers.

This report explores into the main technical details of CVE-2020-0796, including the specific vulnerability in the SMBv3 compression mechanism and ways through which attackers can gain unauthorized access via exploiting the problem. Additionally, there is a detailed plan for demonstrating CVE-2020-0796 in a controlled environment with stepwise instructions on setting up a vulnerable system and running a proof-of-concept exploit.

Furthermore, the report provides elaborate information on methods to detect systems vulnerable to SMBGhost, including network scanning techniques and log analysis. It also offers extensive advice on mitigation strategies such as applying official patches or even going further with temporary workarounds plus network level protections.

SUMMARY OF THE CVE:

CVE-2020-0796, also known as SMBGhost, is a critical vulnerability in the Microsoft Server Message Block 3.1.1 (SMBv3) protocol implementation in certain versions of Microsoft Windows. This vulnerability is a buffer overflow flaw that exists in the way SMBv3 handles compressed data. Exploiting this vulnerability allows an unauthenticated attacker to execute arbitrary code on the target system, potentially leading to a full system compromise. This vulnerability was disclosed in March 2020 and received a CVSS base score of 10.0, indicating the highest severity level (NVD - Cve-2020-0796, n.d.).

AFFECTED SYSTEMS:

- The vulnerability affects the following Windows versions (Security Update Guide - Microsoft Security Response Center, n.d.)
- Windows 10 Version 1903 (32-bit, x64-based, and ARM64-based systems)
- Windows 10 Version 1909 (32-bit, x64-based, and ARM64-based systems)
- Windows Server, version 1903 and 1909 (Server Core installation).

TECHNICAL DETAILS

The vulnerability lies in the way SMBv3 handles compressed data packets. SMBv3 introduced a new compression feature to improve performance, but this feature contained a critical flaw in its implementation.

Specifically, the issue occurs in the decompression routine of the srv2.sys driver. When processing a maliciously crafted compression transform header, the function fails to properly validate the input length of compressed data packets, leading to an integer overflow. This overflow results in a miscalculation of the required buffer size for decompression, potentially allowing an attacker to overwrite memory beyond the allocated buffer (Carroll et al., 2024).

Affected Components:

- Protocol: Server Message Block (SMB) version 3.1.1
- Driver: srv2.sys (implements server-side SMB 2.x and SMB 3.x protocol)

Affected Functions:

- SMBv3 client: SrvNet!ReceiveCompound
- SMBv3 server: Srv2!Srv2DecompressData

VULNERABILITY MECHANISM:

The vulnerability stems from an integer overflow in the decompression function when processing the "compression transform" header of an SMB message. This header contains crucial fields:

- Protocol ID (4 bytes)
- Original Size (4 bytes)
- Compressed Size (4 bytes)
- Compression Algorithm (2 bytes)
- Offset (2 bytes)

The flaw occurs in the following sequence:

- The srv2.sys driver reads the "Original Size" and "Compressed Size" fields.
- It calculates the required decompression buffer size based on these values.
- Due to improper validation, an integer overflow occurs during this calculation. This results in allocating an insufficiently small buffer for decompression. During decompression, data exceeds the allocated buffer, causing a buffer overflow (Carroll et al., 2024).

PLAN FOR EXPLOITATION

This demonstration of the SMBGhost vulnerability requires a target (victim) machine and an attacker machine, with the victim's firewall disabled. the process starts with reconnaissance via Nmap that scans target IP concentrating on port 445/TCP. After this ButrintKomoni's Python script is used to do vulnerability scan (ButrintKomoni, n.d.). The vulnerability is then confirmed by attempting to crash the target system using Jiansiting's script, highlighting the critical nature of this flaw (Jiansiting, n.d.).

For remote code execution, ZecOps' exploit is utilized To perform remote code execution, ZecOps provides an exploit. Prior to running SMBleedingGhost.py script, prepare for it by executing calc_target_offset.bat on victim's system to get offset value. Attacker then sets up netcat to listen for incoming connections. Finally, another Windows system is used to execute the exploit using SMBleedingGhost.py script (Jamf, n.d.). While the initial attempt may crash the target, subsequent tries should succeed in achieving remote code execution.

MITIGATIONS

The SMBGhost vulnerability (CVE-2020-0796) poses a significant threat to systems utilizing SMBv3. To effectively mitigate this risk, a multi-layered security approach is necessary. The primary and most effective mitigation is to apply the latest security updates from Microsoft.

- Use Windows Update to install security updates or cumulative updates released in March 2020 and beyond.
- Ensure automatic updates are enabled for all systems.

The next method would focus on Network level protection. We can implement strict network controls to limit the exposure of smb services in the system by configuring Firewall.

- Block inbound and outbound SMB traffic (TCP port 445) at the network perimeter.
- Use Windows Firewall with Advanced Security to create rules blocking SMB traffic on endpoints.
- Implement VLANs or network zones to isolate systems that require SMB access.
- Use jump boxes or bastion hosts for administrative access to SMB services.

Decrease exposure of the SMB service discovery to external connections by disabling the SMBv3 compression by executing this PowerShell command (Prathap, n.d.):

```
Set-ItemProperty -Path
"HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters"
DisableCompression -Type DWORD -Value 1 -Force
```

However this isn't a complete fix , it can only mitigate the risk. For a more robust and scalable solution, deploying this configuration change through Group Policy Objects (GPO) is recommended. Group policy objects (GPOs) are a way to manage settings across many Windows machines in one place(CVE-2020-0796: SMBV3 "Wormable" Remote Code Execution Vulnerability, 2023).

- Create a GPO using the following command in PowerShell:

```
New-GPO -Name "Disable SMBv3 Compression" -Comment "GPO to disable
SMBv3 compression to mitigate CVE-2020-0796"
```

- Set the registry key and value for the GPO:

```
Set-GPRegistryValue
-Name "Disable SMBv3 Compression" -Key
"HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters "
-ValueName "DisableCompression" -Type DWORD -Value 1
```

DETECTION:

Network-Based Detection DPI:

- Implement DPI on network traffic, focusing on SMB communication (TCP port 445) (What Is SMB | What Is SMB Port Numbers 135 and 445, 2024).
- Look for patterns in SMB packets that indicate exploitation attempts:
- Abnormally large "Original Size" values in compression transform headers.
- Mismatched "Original Size" and "Compressed Size" values.
- Use intrusion detection/prevention systems with custom signatures.

Network Flow Analysis:

- Monitor SMB traffic patterns for anomalies such as sudden increases in SMB traffic volume.
- Unusual source-destination pairs for SMB communication
- Implement machine learning algorithms to detect deviations from baseline SMB traffic patterns.

Protocol Analysis:

- Analyse SMB protocol behaviours.
- Look for compression usage in environments where it's not typically used.Use tools like Wireshark with custom dissectors for SMBv3 compression.

File Integrity Monitoring:

- Monitor critical system files, especially those related to SMB functionality:
- Watch for unexpected modifications to srv2.sys
- Track changes in SMB-related registry keys
- Implement real-time file integrity monitoring solutions.

SMB Honeypots:

- Deploy SMB honeypots that mimic vulnerable systems (Ebrahimi, 2021).
- Configure honeypots to appear as unpatched Windows systems.
- Monitor all connection attempts and payloads sent to these honeypots.

Network Deception:

- Implement network deception techniques:
- Deploy decoy systems that appear vulnerable to CVE-2020-0796.
- Monitor all interactions with these decoy systems. Use deception technology to detect reconnaissance and exploitation attempts.

REFERENCES:

ButrintKomoni. (n.d.). *GitHub - ButrintKomoni/cve-2020-0796: Identifying and Mitigating the CVE-2020-0796 flaw in the fly*. GitHub. https://github.com/ButrintKomoni/cve-2020-0796.git

Carroll, E., Laulheret, P., McGrath, K., & Povolny, S. (2024, February 20). *SMBGHost - Analysis of CVE-2020-0796*. McAfee Blog. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/smbghost-analysis-of-cve-2020-0796/\

CVE-2020-0796: SMBV3 "Wormable" Remote Code Execution Vulnerability. (2023, September 21). TrustedSec. https://trustedsec.com/blog/cve-2020-0796-smbv3-wormable-remote-code-execution-vulnerability

Ebrahimi, K. (2021, February 24). *How to set up a Samba Honeypot (SMB) and lure attackers*. Intrix Cyber Security. https://intrix.com.au/articles/samba-honeypot-smb/

Jamf. (n.d.). *GitHub - jamf/CVE-2020-0796-RCE-POC: CVE-2020-0796 Remote Code Execution POC*. GitHub. https://github.com/ZecOps/CVE-2020-0796-RCE-POC.git

Jiansiting. (n.d.). *GitHub - jiansiting/CVE-2020-0796*. GitHub. https://github.com/jiansiting/CVE-2020-0796.git

NVD - cve-2020-0796. (n.d.). https://nvd.nist.gov/vuln/detail/cve-2020-0796

Prathap. (n.d.). *SMBGHost Vulnerability (CVE-2020-0796)*. SMBGhost Vulnerability (CVE-2020-0796). https://beaglesecurity.com/blog/vulnerability/SMBGhost-Vulnerability-(CVE-2020-0796).html

Security Update Guide - Microsoft Security Response Center. (n.d.). https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-0796

What is SMB | What is SMB Port Numbers 135 and 445. (2024, February 6). MonoVM.com. https://monovm.com/blog/what-is-smb-port/#:~:text=Port%20445%20is%20used%20for,it%20in%20the%20same%20manner.