SMBGhost Vulnerability Scanner (CVE-2020-0796) Report

✔ 172.16.21.200

Summary

Overall risk level:

High

Risk ratings:

High:	1
Medium:	0
Low:	0
Info:	0

Scan information:

Start time:	2020-03-15 20:38:00 UTC+02
Finish time:	2020-03-15 20:38:01 UTC+02
Scan duration:	1 sec
Tests performed:	1/1
Scan status:	Finished

Findings

Possibly vulnerable to SMBGhost CVE-2020-0796 Remote Code Execution (port 445)

We have detected the following configuration on the SMB server of the target host:

SMB Version: **3.1.1**
SMB Compression: **enabled**

Details

Risk description:
It is possible that the target Windows host is affected by a Remote Code Execution vulnerability (CVE-2020-0796, aka SMBGhost, CoronaBlue) in the file sharing service. The vulnerability is caused by a bounds checking error in the implementation of the SMBv3 compression capability in Windows 10 and Windows Server 1903/1909.

Please note that this tool detects only if SMBv3.1.1 is used and if SMBv3 compression is enabled. In case of patched Windows 10 machines, this technique will provide **false positive** results. However, if any of these settings are not detected (SMBv3.1.1 and compression), the results are reliable and the system is not vulnerable to SMBGhost.
To reliably check if the system is patched, you should locally verify if KB4551762 is installed on the Windows host.

The risk exists that an attacker exploits this vulnerability to gain remote code execution on the target machine or cause denial of service (blue screen of death).

Recommendation:
We recommend applying the Microsoft cumulative update KB4551762, which fixes this vulnerability.
There is also a workaround for mitigating this issues. You can disable SMBv3 compression by issuing the following PowerShell command:

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

References:
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0796
https://www.exploit-db.com/exploits/48216
https://github.com/eerykitty/CVE-2020-0796-PoC

Scan coverage information

List of tests performed (1/1)

- ✔ Scanning for SMBGhost CVE-2020-0796 vulnerability...

Scan parameters

Target:	172.16.21.200
Port:	445