National Cyber Security Centre

2003110048-NCSC

A part of **Department of Communications, Climate Action & Environment**

NCSC Advisory

Critical Remote Code Execution (RCE) Vulnerability in
Microsoft Server Message Block 3 (SMBv3)
CVE-2020-0796
2020-03-11
Updated 2020-03-12

Status: TLP-WHITE

NCSC

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

Traffic Light Protocol

This document is classified using Traffic Light Protocol. Recipients may share TLP: WHITE information freely, without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. **Please treat this document in accordance with the TLP assigned.**

Technical Detail

1. Overview

Threat Type	Remote code execution vulnerability in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests.
Systems Affected	• Windows 10 Version 1903 for 32-bit Systems • Windows 10 Version 1903 for ARM64-based Systems • Windows 10 Version 1903 for x64-based Systems • Windows 10 Version 1909 for 32-bit Systems • Windows 10 Version 1909 for ARM64-based Systems • Windows 10 Version 1909 for x64-based Systems • Windows Server, version 1903 (Server Core installation) • Windows Server, version 1909 (Server Core installation) (Update 12/03/20) Microsoft confirms that the vulnerability only exists in a new feature on those operating systems. Older versions do not offer support to SMBv3.1.1 compression
Impact	Successful exploitation of the vulnerability may enable the attacker to execute arbitrary code on targetted SMB Server and SMB Clients.
Recommendations	CSIRT-IE recommends that system administrators apply update KB4551762 against this vulnerability

2. Description

On Tuesday 10th March, Microsoft informed members of the Microsoft Active Protections Programme that Server Message Block 3 (SMBv3) is vulnerable to a buffer overflow exploit that could allow remote execution of arbitrary code, and provided details in CVE-2020-0795.

This vulnerability is associated with how SMBv3 handles compression of its data packets, and it allows

remote, unauthenticated attackers that exploit it to execute arbitrary code within the context of the application.

Microsoft describes this vulnerability as “wormable”. Wormable vulnerabilities in SMB have been exploited in recent years, most notably during the Wannacry outbreak that leveraged weaknesses in SMBv1. As of the time of writing, attacks exploiting CVE-2020-0795 have not been observed.

An unauthenticated attacker can exploit this vulnerability by sending a crafted packet to a targeted SMBv3 server. To exploit against a client, an attacker would have to induce a client into connecting to a preconfigured, malicious SMB server.

3. Mitigation - Update

1. **Apply relevant update**

   Microsoft has released update KB4551762 on March 12.
   KB4551762 can be installed by checking for updates via Windows Update or by manually downloading it for your Windows version from the Microsoft Update Catalog. Details are at `https://support.microsoft.com/en-ie/help/4551762/windows-10-update-kb4551762`

   Microsoft have recommended two workarounds; disable SMBv3 Compression and restrict SMB traffic at the enterprise perimeter firewall.

   It is not necessary to disable SMBv3 Compression once the update has been applied. However, it is best practice to restrict SMB traffic at perimeter.

2. **Restrict SMB traffic at the enterprise perimeter firewall**

   TCP port 445 is used to initiate a connection with the affected component. Blocking this port at the network perimeter firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability. This can help protect networks from attacks that originate outside the enterprise perimeter. Blocking the affected ports at the enterprise perimeter is the best defense to help avoid Internet-based attacks.
   However, systems could still be vulnerable to attacks from within their enterprise perimeter.

   - Block outbound SMB connections (TCP port 445 for SMBv3) from the local network to the WAN.
   - Ensure that inbound SMB connections from the Internet are not allowed to connect to an enterprise LAN.
   - Consider enabling alerts on perimeter firewall for attempts to use port 445 from or to external resources.
   - Please see the following link for **Microsoft’s recommendations for controlling SMB traffic**

3. **Disable SMBv3 Compression:**

   - Compression can be disabled to block unauthenticated attackers from exploiting the vulnerability against an SMBv3 Server with the PowerShell command below:

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

- This workaround can be disabled with the powershell command below:

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\
LanmanServer\Parameters" DisableCompression -Type DWORD -Value 0 -Force
```

- **This workaround does not protect exploitation of SMB clients**

Feedback and Reporting

NCSC-IE wishes to offer whatever assistance it can in relation to this incident and is willing to work with the relevant parties to further understand the current threat. NCSC-IE would also request any feedback in relation to this incident as regards the relevance and accuracy of the information provided. NCSC-IE would appreciate notification of any attempt to exploit CVE-2020-0796.