CVE-2020-1206 | Windows SMBv3 信息泄漏漏洞通告

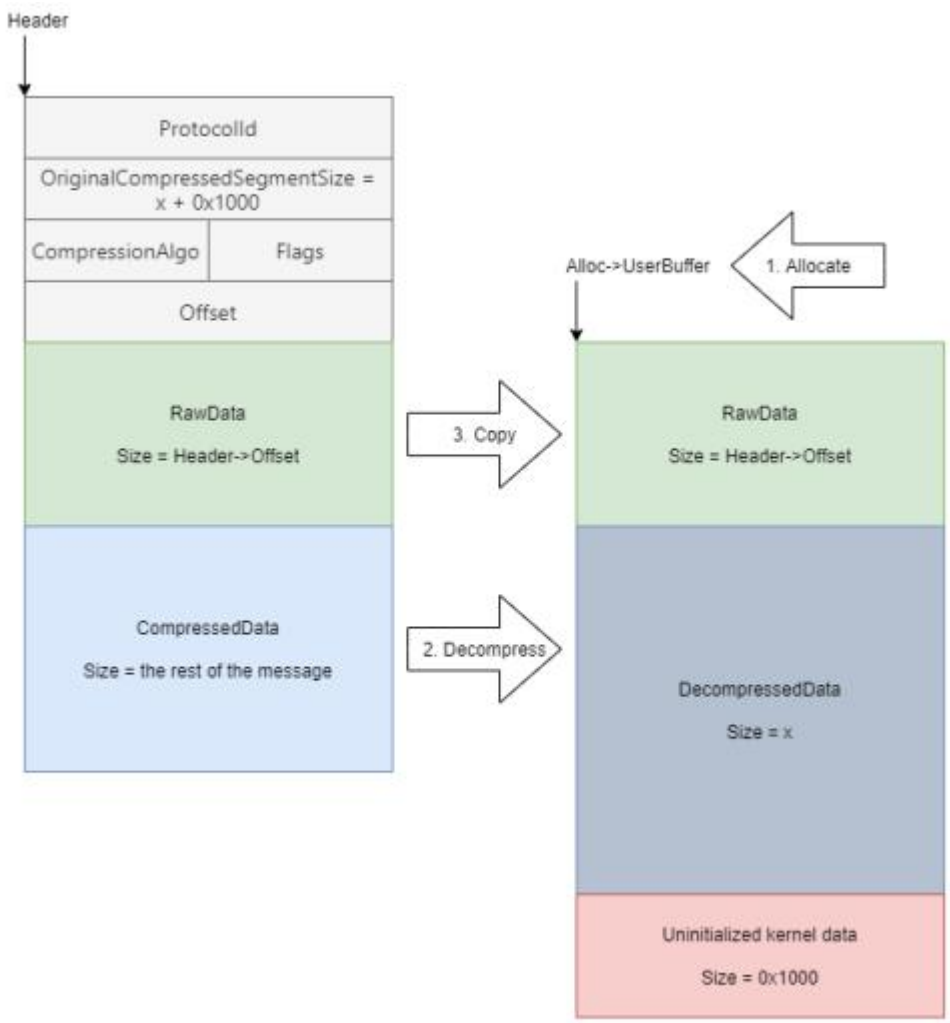
0x00 漏洞概述

CVE ID	CVE-2020-1206	时 间	2020-06-12
类 型	II	等 级	高危
远程利用	是	影响范围	

0x01 漏洞详情

微软于周二发布了 6 月安全更新补丁，修复了 129 个漏洞。其中包括一个 Windows SMBv3 客户端/服务器信息泄漏漏洞（CVE-2020-1206），研究人员将其命名为 SMBleed。该漏洞位于 SMB 的解压缩函数中，与 SMBGhost 或 EternalDarkness 漏洞(CVE-2020-0796)位于同一函数中，攻击者利用该漏洞无需身份验证即可远程泄漏内核内存信息，如果与之前爆出的 CVE-2020-0796 漏洞结合，可以实现远程代码执行。

要利用针对服务器的漏洞，未经身份验证的攻击者可以将特制数据包发送到目标 SMBv3 服务器。要利用针对客户端的漏洞，未经身份验证的攻击者将需要配置恶意的 SMBv3 服务器，并说服用户连接到该服务器。由于 SMB 的解压缩函数 Srv2DecompressData 在处理发送给目标 SMBv3 服务器消息请求时存在问题，从而使攻击者可以读取未初始化的内核内存并修改压缩功能。



关于漏洞利用的 PoC，参考链接如下：

SMBleed POC：https://github.com/ZecOps/CVE-2020-1206-POC。

SMBleed 与 SMBGhost 结合的 POC：https://github.com/ZecOps/CVE-2020-0796-RCE-POC。

0x02 影响范围

以下是 CVE-2020-1206 漏洞受影响的系统版本：
Windows 10 Version 1909 for 32-bit Systems Windows
10 Version 1909 for x64-based Systems Windows 10
Version 1909 for ARM64-based Systems
Windows Server, version 1909 (Server Core installation)

Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1903 for x64-based Systems
Windows 10 Version 1903 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Server, version 2004 (Server Core installation)

0x03 处置建议

微软已经发布补丁更新，下载链接：

https://catalog.update.microsoft.com/v7/site/Search.aspx?q=KB4557957

禁用 SMBv3 压缩

您可以使用以下 PowerShell 命令禁用压缩功能，以阻止未经身份验证的攻击者利用 SMBv3 服务器的漏洞。

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

注意：

1. 进行更改后，无需重启。
2. 此解决方法不能阻止利用 SMB 客户端；保护客户端请参考以下链接：
   https://support.microsoft.com/zh-cn/help/3185535/preventing-smb-traffic-from-lateral-connections
3. Windows 或 Windows Server 尚未使用 SMB 压缩，并且禁用 SMB 压缩不会产生负面的性能影响。

你可以使用下面的 PowerShell 命令禁用该变通方法。

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

注意：禁用此解决方法后，无需重启。

0x04 相关新闻

https://securityaffairs.co/wordpress/104584/hacking/microsoft-vulnerability-smbleed.html?utm_source=rss&utm_medium=rss&utm_campaign=microsoft-vulnerability-smbleed

0x05 参考链接

https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1206
https://blog.zecops.com/vulnerabilities/smbleedingghost-writeup-chaining-smbleed-cve-2020-1206-with-smbghost/

0x06 时间线

2020-06-09　微软更新漏洞补丁

2020-06-12　VSRC 发布漏洞通告