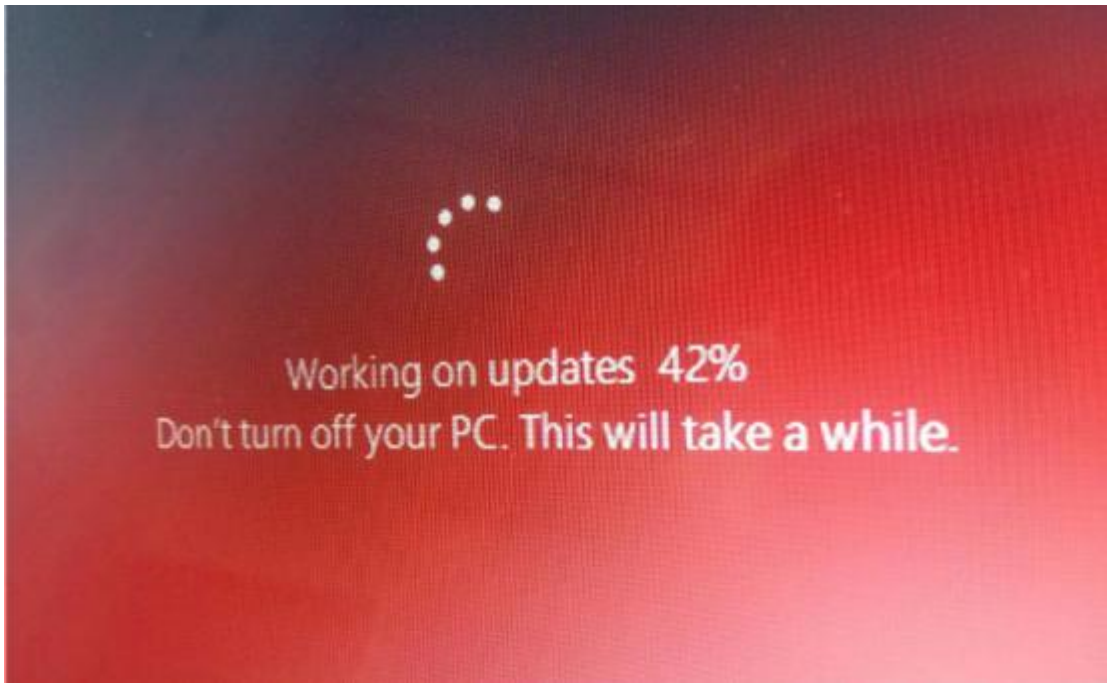
CVE-2020-1301 | Windows SMB v1 远程代码执行漏洞通告

0x00 漏洞概述

CVE ID	CVE-2020-1301	时 间	2020-06-10
类 型	RCE	等 级	中危
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 SMB 远程代码执行漏洞（CVE-2020-1301）,尽管本月更新的漏洞数量很多，但在 Microsoft 今天发布补丁之前，还没有发现被利用的漏洞。建议管理员尽快部署更新。

Server Message Block（SMB）是为计算机提供身份验证以访问服务器上打印机和文件系统的组件。该漏洞源于 Microsoft SMB 1.0 (SMBv1) 服务器在处理某些请求的方法中存在错误，导致成功利用此漏洞的攻击者可以在目标系统上执行任意代码。

另外的永恒之蓝就是利用 SMB v1 漏洞，建议关闭 SMB v1，想要触发此漏洞需要先通过身份认证，危害等级属于中危。

0x02 影响范围

以下是 CVE-2020-1301 漏洞受影响的系统版本：

Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 for x64-based Systems
Windows Server, version 1803 (Server Core Installation)
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server 2019
Windows Server 2019 (Server Core installation)
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 1709 for 32-bit Systems
Windows 10 Version 1709 for x64-based Systems
Windows 10 Version 1709 for ARM64-based Systems
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 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016
Windows Server 2016 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core

installation)
Windows Server 2012
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 2004 for x64-based Systems
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 2004 for 32-bit Systems
Windows 10 Version 2004 for ARM64-based Systems

0x03 处置建议

建议禁用 SMB v1

对于运行 Windows Vista 和更高版本的用户，请参考 Microsoft 知识库文章 2696547。

运行 Windows 8.1 或 Windows Server 2012 R2 及更高版本的客户端操作系统：

1. 打开控制面板，单击“程序”，然后单击“打开或关闭 Windows 功能”。
2. 在“Windows 功能”窗口中，清除“SMB 1.0 / CIFS 文件共享支持”复选框，然后单击“确定”关闭该窗口。
3. 重新启动系统。

对于服务器操作系统：

1. 打开服务器管理器，然后单击“管理”菜单，然后选择“删除角色和功能”。
2. 在“功能”窗口中，清除“SMB 1.0 / CIFS 文件共享支持”复选框，然后单击“确定”关闭该窗口。
3. 重新启动系统。

此解决方法将导致 SMB v1 协议将在目标系统上被禁用。

0x04 相关新闻

https://www.zdnet.com/article/microsoft-june-2020-patch-tuesday-fixes-129-vulnerabilities/#ftag=RSSbaffb68

0x05 参考链接

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1301

https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3
https://portal.msrc.microsoft.com/zh-cn/security-guidance

0x06 时间线

2020-06-09　微软更新漏洞补丁

2020-06-10　VSRC 发布漏洞通告