Microsoft 发布 2020 年 2 月安全更新

2 月 11 日，微软发布了 2020 年 2 月份的月度例行安全公告，修复了其多款产品存在的 373 个安全漏洞。受影响的产品包括：Windows 10 1909 & WindowsServer v1909（71 个）、Windows 10 1903 & WindowsServer v1903（72 个）、Windows 10 1809 & WindowsServer 2019（69 个）、Windows 8.1 & Server 2012 R2（49 个）、Windows RT 8.1（48 个）、Windows Server 2012（49 个）、Microsoft Edge (HTML)（7 个）、Internet Explore（3 个）和 Microsoft Office-related software（5 个）。

利用上述漏洞，攻击者可以获取敏感信息，提升权限，欺骗，绕过安全功能限制，执行远程代码，或进行拒绝服务攻击等。CNVD 提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

CVE 编号	公告标题和摘要	最高严重等级和漏洞影响	受影响的软件
CVE-2020-0738	**Media Foundation 内存破坏漏洞** 当 Windows Media Foundation 未能正确地处理内存中的对象时，存在内存破坏漏洞。成功利用此漏洞的攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。 攻击者可以通过多种方式利用此漏洞，例如说服用户打开精心编制的文档，或说服用户访问恶意网页。 安全更新通过更正 Windows Media Foundation 如何处理内存中的对象来解决此漏洞。	严重 远程执行代码	Windows 10 Server 2016 Server 2019 Server, version 1803 Server, version 1903 Server, version 1909 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-0689	**Microsoft Secure Boot 安全功能绕过漏洞** Secure Boot 存在安全功能绕过漏洞。成功利用此漏洞的攻击者可以绕过安全引导并加载不受信任的软件。要利用此漏洞，攻击者可以运行构建的应用程序。 安全更新通过阻止易受攻击的第三方引导加载程序来解决该漏洞。	重要 绕过安全功能	Windows 10 Server 2016 Server 2019 Server, version 1803 Server, version 1903 Server, version 1909 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-0681	**Remote Desktop Client 远程代码执行漏洞** 当用户连接到恶意服务器时， Windows Remote Desktop Client 存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在连接客户端的计算机上执行任意代码。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。 要利用此漏洞，攻击者需要控制服务器，然后说服用户连接到该服务器。攻击者无法强迫用户连接到恶意服务器，他们需要通过社会工程、DNS 中毒或使用中间人（MITM）技术诱骗用户连接。攻击者还可能危害合法服务器，在其上托管恶意代码，并等待用户连接。	严重 远程执行代码	Windows 10 Server 2016 Server 2019 Server, version 1803 Server, version 1903 Server, version 1909 Windows 8.1 Server 2012 Server 2012 R2

	此更新通过更正 Windows 远程桌面客户端处理连接请求的方式来解决此漏洞。		
CVE-2020-0683/0686	**Windows Installer 权限提升漏洞** 当 MSI 包处理符号链接时，Windows Installer 中存在权限提升漏洞。成功利用此漏洞的攻击者可以绕过访问限制来添加或删除文件。 要利用此漏洞，攻击者首先必须登录到系统。然后，攻击者可以运行巧尽心思构建的应用程序，利用此漏洞并添加或删除文件。 安全更新通过修改 Windows 安装程序处理重分析点的方式来解决该漏洞。	重要 特权提升	Windows 10 Server 2016 Server 2019 Server, version 1803 Server, version 1903 Server, version 1909 Windows 8.1 Server 2012 Server 2012 R2
CVE-2020-0674	**Scripting Engine 内存破坏漏洞** Internet Explorer 中处理内存中对象的方式存在远程代码执行漏洞。该漏洞可能会破坏内存，使得攻击者可以在当前用户的上下文中执行任意代码。成功利用此漏洞的攻击者可以获得与当前用户相同的用户权限。如果当前用户使用管理用户权限登录，则成功利用此漏洞的攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。	严重 远程执行代码	Internet Explorer 10 Internet Explorer 9 Internet Explorer 11
CVE-2020-0706	**Microsoft Browser 信息泄露漏洞** Microsoft browsers 处理交叉原点请求的方式存在信息泄露漏洞。成功利用此漏洞的攻击者可以确定受影响浏览器中所有网页的来源。	重要 信息泄露	Microsoft Edge (HTML) Internet Explorer 9 Internet Explorer 10 Internet Explorer 11
CVE-2020-0759	**Microsoft Excel 远程代码执行漏洞** 当软件未能正确处理内存中的对象时，Microsoft Excel 中存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在当前用户的上下文中运行任意代码。如果当前用户使用管理用户权限登录，则攻击者可以控制受影响的系统。然后，攻击者可以安装程序；查看、更改或删除数据；或创建具有完全用户权限的新帐户。将帐户配置为在系统上拥有较少用户权限的用户可能比使用管理用户权限操作的用户受影响更小。 安全更新通过更正 Microsoft Excel 如何处理内存中的对象来解决此漏洞。	重要 远程执行代码	Office 2019 Office 365 ProPlus Excel 2010 Excel 2013 Excel 2016 Office 2016 for Mac Office 2019 for Mac
CVE-2020-0693	**Microsoft Office SharePoint XSS 漏洞** 当 Microsoft SharePoint Server 未能正确对受影响的 SharePoint 服务器进行制作的 Web 请求时，存在跨站脚本（XSS）漏洞。经过身份验证的攻击者可以通过向受影响的 SharePoint 服务器发送构建的请求来利用此漏洞。 成功利用此漏洞的攻击者可以对受影响的系统执行跨站脚本攻击，并在当前用户的安全上下文中运行脚本。这些攻击可使攻击者读取未经授权读取的内容，使用受害	重要 欺骗	SharePoint Enterprise Server 2016 SharePoint Server 2019 Mitigations SharePoint Server 2013

	者身份代表用户在 SharePoint 网站上执行更改权限和删除内容等操作，并在用户浏览器中插入恶意内容。安全更新通过帮助确保 SharePoint 服务器正确地清理 web 请求来解决该漏洞。		

参考信息：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/adv990001

https://docs.microsoft.com/en-us/windows/deployment/update/servicing-stackupdates#why-should-servicing-stack-updates-be-installed-and-kept-up-to-date