中共内蒙古自治区委员会网络安全和信息化委员会办公室 文件

国家计算机网络与信息安全管理中心内蒙古分中心

内党网安通〔2019〕1号

关于“微软产品2019年2月安全漏洞”网络安全预警的通报

各盟市委网信办，自治区各部门和有关单位：

近日，微软发布了2019年2月月度安全公告，公布了其多款产品存在的安全漏洞。受本次漏洞影响的系统和软件包括Windows 10 1809、Windows Server2019、Windows 10 1803、WindowsServer v1803、Windows 10 1709、WindowsServer v1709、Windows RT 8.1、Windows Server 2012、Windows 8.1、Server 2012 R2、Windows Server 2008、Windows 7、Windows Server 2008R2、Internet Explorer、Microsoft Edge和Office。利用这些安全漏洞，攻击者可以获取敏感信息，提升权限，绕过安全功能限制，执行远程代码，或发起拒绝服务攻击等。

微软已于2月发布了相关漏洞的更新补丁。请各地区、

各部门和有关单位结合自身实际情况及时排查，在确保网络和信息系统安全稳定运行的前提下，尽快下载并安装更新补丁，避免引发网络安全事件。

联系人及电话：李景辉　0471-4826732

杨佳楠　0471-6684114

附件：微软漏洞详细情况表

中共内蒙古自治区委员会网络安全和信息化委员会办公室

国家计算机网络与信息安全管理中心内蒙古分中心

2019年2月25日

附件

微软漏洞详细情况表

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-2019-0630	**Microsoft Windows SMB Server 远程代码执行漏洞** Microsoft Server Message Block 2.0（smbv2）服务器处理某些请求时存在远程代码执行漏洞。为了利用该漏洞，经过身份验证的攻击者可以向目标 smbv2 服务器发送精心设计的数据包。	重要 远程执行代码	Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2008 Windows Server 2012 Windows Server 2016 Windows Server 2019 Server, version 1709 Server, version 1803 Windows 8.1 Windows 10 Windows 7
CVE-2019-0626	**Microsoft Windows DHCP Server 远程代码执行漏洞** 当攻击者向 DHCP 服务器发送精心设计的数据包时，Windows Server DHCP 服务中存在内存破坏漏洞。成功利用该漏洞的攻击者可以在 DHCP 服务器上运行任意代码。	严重 远程执行代码	Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2008 Windows Server 2012 Windows Server 2016 Windows Server 2019 Server, version 1709 Server, version 1803 Windows 8.1 Windows 10 Windows 7
CVE-2019-0662	**Microsoft Windows GDI+ 组件远程代码执行漏洞** 攻击者可以通过多种方式利用该漏洞：在基于 Web 的攻击场景中，攻击者可以托管一个专门设计用于利用该漏洞的网站，然后说服用户查看该网站。在文件共享攻击场景中，攻击者可以提供专门设计的文档文件，该文件旨在利用漏洞，然后说服用户打开文档文件。	严重 远程执行代码	Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2008 Windows Server 2012 Windows Server 2016 Windows Server 2019 Server, version 1709 Server, version 1803 Windows 8.1 Windows 10 Windows 7

CVE-2019-0625	**Microsoft Windows Jet 数据库引擎远程代码执行漏洞** 当 Windows Jet 数据库引擎未能正确地处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在受害者的系统上执行任意代码。攻击者可以通过诱使受害者打开精心编制的文件来利用此漏洞。	重要 远程执行代码	Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2008 Windows Server 2012 Windows Server 2016 Windows Server 2019 Server, version 1709 Server, version 1803 Windows 8.1 Windows 10 Windows 7
CVE-2019-0636	**Microsoft Windows 本地信息泄露漏洞** 当 Windows 不正确地公开文件信息时，存在信息漏洞。成功利用该漏洞可使攻击者读取磁盘上文件的内容。要利用该漏洞，攻击者必须登录受影响的系统并运行专门设计的应用程序。通过更改 Windows 公开文件信息的方式来解决该漏洞。	重要 信息泄露	Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2008 Windows Server 2012 Windows Server 2016 Windows Server 2019 Server, version 1709 Server, version 1803 Windows 8.1 Windows 10 Windows 7
CVE-2019-0606	**Microsoft Internet Explorer 远程内存破坏漏洞** 攻击者可以托管一个精心设计的网站，该网站旨在通过受影响的 Microsoft 浏览器利用该漏洞，然后说服用户查看该网站。	严重 远程执行代码	Internet Explorer 11
CVE-2019-0607	**Microsoft Edge Chakra Scripting Engine 远程内存破坏漏洞** 攻击者可以托管一个精心设计的网站，该网站旨在通过受影响的 Microsoft 浏览器利用该漏洞，然后说服用户查看该网站。攻击者还可以在承载浏览器呈现引擎的应用程序或 Office 文档中嵌入标记为“初始化安全”的 ActiveX 控件。	严重 远程执行代码	Microsoft Edge ChakraCore
CVE-2019-0594	**Microsoft SharePoint Server 远程代码执行漏洞** 当软件无法检查应用程序包的源标记时，Microsoft SharePoint 中存在远程代码执行漏洞。成功利用漏	严重 远程执行代码	SharePoint Server 2010 SharePoint Foundation 2013 SharePoint Enterprise Server 2016 SharePoint Server 2019

	洞的攻击者可以运行 SharePoint 应用程序池和 SharePoint 服务器场帐户上下文中的任意代码。利用此漏洞需要用户将精心设计的 SharePoint 应用程序包上载到受影响的 SharePoint 版本。		
CVE-2019-0671	**Microsoft Office Access Connectivity Engine 远程代码执行漏洞** 当 Microsoft Office Access 连接引擎未能正确地处理内存中的对象时，存在远程代码执行漏洞。成功利用此漏洞的攻击者可以在受害者系统上执行任意代码。攻击者可以通过诱使受害者打开精心编制的文件来利用此漏洞。	重要 远程执行代码	Office 2010/2013/2016/2019 Office 365 ProPlus

参考链接：

https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/51503ac5-e6d2-e811-a983-000d3a33c573