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 文件

内党网安通〔2019〕16号

关于“微软产品2019年11月安全漏洞”网络安全预警的通报

各盟市及满洲里、二连浩特市委网信办，自治区各有关部门和单位：

近日，微软发布了2019年11月份的月度例行安全公告，，修复了其多款产品存在的322个安全漏洞。受影响的产品包括：Windows 10 1903 & WindowsServer v1903（46个）、Windows 10 1809 & WindowsServer 2019（46个）、Windows 10 1803 & WindowsServer v1803（46个）、Windows 8.1 & Server 2012 R2（37个）、Windows RT 8.1（32个）、WindowsServer 2012（37个）、Windows7 and Windows Server 2008 R2（35个）、WindowsServer 2008（31个）、MicrosoftEdge（4个）、

InternetExplorer（2 个）和 Microsoft SharePoint-related software（6 个）。

利用上述漏洞，攻击者可以提升权限，欺骗，绕过安全功能限制，获取敏感信息，执行远程代码或发起拒绝服务攻击等。请各地区、各有关部门和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，避免引发漏洞相关的网络安全事件。

联系人及电话：张　宇　0471-3905371

王　艳　0471-4826732

附件：安全漏洞情况

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 11 月 21 日

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 2019 年 11 月 21 日印发

附件：安全漏洞情况

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-2019-1 38 4	**NETLOGON 安全功能绕过漏洞** NETLogon 消息能够获得会话密钥并签署消息时，存在安全功能绕过漏洞。要利用此漏洞，攻击者可以发送精心编制的身份验证请求。成功利用此漏洞的攻击者可以使用原始用户权限访问其他计算机。通过更改 NTLM 验证网络身份验证消息的方式解决该问题。	重要 绕过安全功能	Windows 10 Windows 7 Windows 8.1 Server 2008 Server 2008 R2 Server 2012 Server 2012 R2 Server 2016 Server, version 1803 Server 2019 Server, version 190 3
CVE-2019-1 397	**Windows Hyper-V 远程代码执行漏洞** 当主机服务器上的 Windows Hyy-V 未能正确验证来自客户操作系统上的身份验证的用户的输入时，存在远程代码执行漏洞。要利用此漏洞，攻击者可以在客户操作系统上运行构建的应用程序，可能会导致 Hyper-V 主机操作系统执行任意代码。成功利用此漏洞的攻击者可以在主机操作系统上执行任意代码。安全更新通过更正 Hyper-V 如何验证客户操作系统用户输入来解决该漏洞。	严重 远程执行代码	Windows 10 Server, version 1803 Server 2019 Server, version 1903 Server 2016 Windows 7 Windows 8.1 Server 2008 Server 2008 R2 Server 2012 Server 2012 R2
CVE-2019-1 419	**OpenType Font Parsing 远程代码执行漏洞** 当 Windows Adobe 类型管理器库未能正确处理精心制作的 OpenType 字体时，在 Microsoft Windows 中存在远程代码执行漏洞。对于除 Windows 10 以外的所有系统，成功利用此漏洞的攻击者都可以远程执行代码。攻击者有多种方法可以利用此漏洞进行攻击，例如说服用户打开精心编制的文档，或者说服用户访问包含巧尽心思构建的嵌入 OpenType 字体的网页。	严重 远程执行代码	Windows 10 Server, version 1803 Server 2019 Server, version 1903 Server 2016 Windows 7 Windows 8.1 Server 2008 Server 2008 R2 Server 2012 Server 2012 R2
CVE-2019-1 429	**Internet Explorer 脚本引擎内存破坏漏洞** Internet Explorer 脚本引擎处理内存对象的方式存在远程代码执行漏洞。该漏洞可破坏内存，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	重要 远程执行代码	Internet Explorer 10 Internet Explorer 9 Internet Explorer 11

	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。		
CVE-2019-1448	**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 软件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 2019 for Mac Office 365 ProPlus Excel 2016 Office 2016 for Mac Excel 2010 Excel 2013
CVE-2019-1443	**Microsoft SharePoint 信息泄漏漏洞** 当微软向 SharePoint 服务器上传专门制作的文件时，ShareSharePoint 中存在信息泄露漏洞。成功利用此漏洞的经过身份验证的攻击者可能会利用 SharePoint 功能获取 SMB 哈希。 安全更新通过更正 SharePoint 如何检查文件内容来解决该漏洞。	重要 信息泄露	SharePoint Enterprise Server 2016 SharePoint Server 2019 SharePoint Foundation 2010 SharePoint Foundation 2013