关于 Microsoft Word 远程代码执行漏洞的紧急预警

广东省网络与信息安全通报中心

2023 年 03 月 07 日

编号：2023008

目录

一、安全预警 2

二、事件信息 2

（一）事件概要 2

（二）漏洞描述 3

（三） 影响范围 4

三、防范建议 5

四、应急处置建议 5

一、安全预警

近期，发现 Microsoft Word 存在远程代码执行漏洞。Microsoft Word 是微软（Microsoft）公司的一套 Office 套件中的文字处理软件。应用范围较广，因此威胁影响范围较大。

请各重点单位高度重视，加强网络安全防护，切实保障网络系统安全稳定运行。

二、事件信息

（一）事件概要

事件名称	Microsoft Word 远程代码执行漏洞 CVE 编号：CVE-2023-21716		
威胁类型	远程代码执行	**威胁等级**	高
受影响的应用版本			
• SharePoint Server Subscription Edition Language Pack • Microsoft 365 Apps for Enterprise for 32-bit Systems • Microsoft Office LTSC 2021 for 64-bit editions • Microsoft SharePoint Server Subscription Edition • Microsoft Office LTSC 2021 for 32-bit editions			

- Microsoft Office LTSC for Mac 2021
- Microsoft Word 2013 Service Pack 1 (64-bit editions)
- Microsoft Word 2013 RT Service Pack 1
- Microsoft Word 2013 Service Pack 1 (32-bit editions)
- Microsoft SharePoint Foundation 2013 Service Pack 1
- Microsoft Office Web Apps Server 2013 Service Pack 1
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2013 Service Pack 1
- Microsoft SharePoint Enterprise Server 2016
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft Office 2019 for Mac
- Microsoft Office Online Server

（二）漏洞描述

Microsoft Word 的 RTF 解析器（wwlib）中存在远程代码执行漏洞，远程攻击者可通过发送带有富文本格式 (RTF) 负载的

文件诱导用户打开来利用此漏洞，成功利用此漏洞可在目标系统上以该用户权限执行任意代码。

（三）影响范围

- SharePoint Server Subscription Edition Language Pack
- Microsoft 365 Apps for Enterprise for 32-bit Systems
- Microsoft Office LTSC 2021 for 64-bit editions
- Microsoft SharePoint Server Subscription Edition
- Microsoft Office LTSC 2021 for 32-bit editions
- Microsoft Office LTSC for Mac 2021
- Microsoft Word 2013 Service Pack 1 (64-bit editions)
- Microsoft Word 2013 RT Service Pack 1
- Microsoft Word 2013 Service Pack 1 (32-bit editions)
- Microsoft SharePoint Foundation 2013 Service Pack 1
- Microsoft Office Web Apps Server 2013 Service Pack 1
- Microsoft Word 2016 (32-bit edition)
- Microsoft Word 2016 (64-bit edition)
- Microsoft SharePoint Server 2019
- Microsoft SharePoint Enterprise Server 2013 Service Pack 1

- Microsoft SharePoint Enterprise Server 2016
- Microsoft 365 Apps for Enterprise for 64-bit Systems
- Microsoft Office 2019 for Mac
- Microsoft Office Online Server

三、防范建议

目前泛微官方已发布安全版本，建议受影响用户及时更新，参考链接如下：

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2023-21716

四、应急处置建议

一旦发现系统中存在漏洞被利用的情况，要第一时间上报我中心，同时开展以下紧急处置：

一是立即断开被入侵的主机系统的网络连接，防止进一步危害；

二是留存相关日志信息；

三是通过“防范建议”加固系统并通过检查确认无相关漏洞后再恢复网络连接。