安全通告

中国网安预警“Microsoft Word 远程代码执行漏洞”，漏洞等级严重，强烈建议及时采取修复或缓解措施以避免受到损失。

漏洞名称： Microsoft Word 远程代码执行漏洞

漏洞编号： CVE-2023-21716

漏洞等级： 严重

漏洞概要：

近期监测到 Microsoft Word 远程代码执行漏洞详情和 POC 已被公开。Microsoft Word 的 RTF 解析器在处理 RTF 文件时，当字体表包含过多字体，会发生越界写入操作，造成堆破坏漏洞。该漏洞 CVSS3 基础评分 9.8，攻击者可通过邮件或其他方式远程发送包含恶意 payload 的 RTF 文档，诱导用户打开或预览文档时会触发漏洞，导致远程代码执行，获取主机权限，机密性、完整性、可用性完全丧失。

经持续跟踪研判，暂未监测到在野利用，短期内可能出现漏洞武器化。攻防实验室已完成调试分析，确认 POC 可导致越界写入。

调试分析:

触发漏洞时的调用栈

```
(9e0.1fd0): Access violation - code c0000005 (first chance)
First chance exceptions are reported before any exception handling.
This exception may be expected and handled.
eax=007554ec ebx=00000001 ecx=000004e4 edx=ffff7ffc esi=19960048 edi=00008002
eip=69e88002 esp=00755490 ebp=007554a4 iopl=0         nv up ei pl nz na po nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00010202
wwlib!DllGetClassObject+0x57cf7:
69e88002 66894c5604      mov     word ptr [esi+edx*2+4],cx ds:002b:19950044=????
0:000> kv
 # ChildEBP RetAddr      Args to Child
WARNING: Stack unwind information not available. Following frames may be wrong.
00 007554a4 69e79467     00755530 00000001 007554ec wwlib!DllGetClassObject+0x57cf7
01 00757938 69e777f3     6a7e517d 03a0e390 0005d400 wwlib!DllGetClassObject+0x4915c
02 00757d44 6aede9dc     00000088 03a0e390 15a3f120 wwlib!DllGetClassObject+0x474e8
03 00757f94 6aede37c     03a0e394 0075e2d4 00759cc8 wwlib!WordMailReact::WordMailReactUser::PUserInstanceG
04 00757fe0 6a0aa674     40080000 00000002 15fad7b0 wwlib!WordMailReact::WordMailReactUser::PUserInstanceG
05 00759730 69b78139     04012000 20080000 00000002 wwlib!DllGetClassObject+0x27a369
06 00759a68 69b6dea9     00000000 ffffffff 00000000 wwlib!FMain+0x222b08
07 00759ae8 69b52b28     00000000 ffffffff 00000000 wwlib!FMain+0x218878
08 0075d0cc 69b5012d     04012000 00000000 00000002 wwlib!FMain+0x1fd4f7
09 0075d180 69d69f7d     04012000 00000000 00000002 wwlib!FMain+0x1faafc
0a 0075e2a4 69d62769     00000000 00000000 00000002 wwlib!FMain+0x41494c
0b 0075f4b0 6cf1225e     6b490714 15d3f870 9fc173e7 wwlib!FMain+0x40d138
0c 0075f564 6cf120a2     0075f584 15d3f870 03a6b828 mso98win32client+0x11225e
0d 0075f598 6cf1201a     00931790 160c7d40 160e0af0 mso98win32client+0x1120a2
0e 0075f628 707aeef3     00931790 160c7d30 00000000 mso98win32client+0x11201a
0f 0075f660 7082bf11     160c7d40 0c16f7e8 0c16f7ec mso20win32client+0x5eef3
```

rtf 文件中字体表格式如下

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  对应文本
00000000   7B 5C 72 74 66 31 7B 0A 7B 5C 66 6F 6E 74 74 62  {\rtf1{.{\fonttb
00000010   6C 7B 5C 66 30 41 3B 7D 0A 7B 5C 66 31 41 3B 7D  l{\f0A;}.{\f1A;}
00000020   0A 7B 5C 66 32 41 3B 7D 0A 7B 5C 66 33 41 3B 7D  .{\f2A;}.{\f3A;}
00000030   0A 7B 5C 66 34 41 3B 7D 0A 7B 5C 66 35 41 3B 7D  .{\f4A;}.{\f5A;}
00000040   0A 7B 5C 66 36 41 3B 7D 0A 7B 5C 66 37 41 3B 7D  .{\f6A;}.{\f7A;}
00000050   0A 7B 5C 66 38 41 3B 7D 0A 7B 5C 66 39 41 3B 7D  .{\f8A;}.{\f9A;}
00000060   0A 7B 5C 66 31 30 41 3B 7D 0A 7B 5C 66 31 31 41  .{\f10A;}.{\f11A
00000070   3B 7D 0A 7B 5C 66 31 32 41 3B 7D 0A 7B 5C 66 31  ;}.{\f12A;}.{\f1
00000080   33 41 3B 7D 0A 7B 5C 66 31 34 41 3B 7D 0A 7B 5C  3A;}.{\f14A;}.{\
00000090   66 31 35 41 3B 7D 0A 7B 5C 66 31 36 41 3B 7D 0A  f15A;}.{\f16A;}.
000000A0   7B 5C 66 31 37 41 3B 7D 0A 7B 5C 66 31 38 41 3B  {\f17A;}.{\f18A;
000000B0   7D 0A 7B 5C 66 31 39 41 3B 7D 0A 7B 5C 66 32 30  }.{\f19A;}.{\f20
000000C0   41 3B 7D 0A 7B 5C 66 32 31 41 3B 7D 0A 7B 5C 66  A;}.{\f21A;}.{\f
000000D0   32 32 41 3B 7D 0A 7B 5C 66 32 33 41 3B 7D 0A 7B  22A;}.{\f23A;}.{
000000E0   5C 66 32 34 41 3B 7D 0A 7B 5C 66 32 35 41 3B 7D  \f24A;}.{\f25A;}
000000F0   0A 7B 5C 66 32 36 41 3B 7D 0A 7B 5C 66 32 37 41  .{\f26A;}.{\f27A
00000100   3B 7D 0A 7B 5C 66 32 38 41 3B 7D 0A 7B 5C 66 32  ;}.{\f28A;}.{\f2
00000110   39 41 3B 7D 0A 7B 5C 66 33 30 41 3B 7D 0A 7B 5C  9A;}.{\f30A;}.{\
00000120   66 33 31 41 3B 7D 0A 7B 5C 66 33 32 41 3B 7D 0A  f31A;}.{\f32A;}.
```

其中”\f”后面的数字就是 font id，处理代码如下

```
69e87ff5 0fbf0e          movsx   ecx, word ptr [esi]
69e87ff8 0fbf5602        movsx   edx, word ptr [esi+2]
69e87ffc 8d1451          lea     edx, [ecx+edx*2]
69e87fff 668b08          mov     cx, word ptr [eax]
69e88002 66894c5604      mov     word ptr [esi+edx*2+4], cx
```

通过 movsx 指令读取 font id，movsx 为带符号扩展的传送指令，读取的过程中，被传送的值会持续增长，当增长到 0x8000 以后，edx 的高 4 字节会被扩展为 0xffff

```
0:000> g
Breakpoint 1 hit
eax=00b84dfc ebx=00000001 ecx=00007ff7 edx=ffffffff esi=1b20d480 edi=00007ff8
eip=69e87ff8 esp=00b84da0 ebp=00b84db4 iopl=0         nv up ei pl nz na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000206
wwlib!DllGetClassObject+0x57ced:
69e87ff8 0fbf5602        movsx   edx,word ptr [esi+2]     ds:002b:1b20d482=7ff8
0:000> p
eax=00b84dfc ebx=00000001 ecx=00007ff7 edx=00007ff8 esi=1b20d480 edi=00007ff8
eip=69e87ffc esp=00b84da0 ebp=00b84db4 iopl=0         nv up ei pl nz na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000206
wwlib!DllGetClassObject+0x57cf1:
69e87ffc 8d1451          lea     edx,[ecx+edx*2]
0:000> g
Breakpoint 1 hit
eax=00b84dfc ebx=00000001 ecx=00007ff8 edx=0000fff0 esi=1b20d480 edi=00008002
eip=69e87ff8 esp=00b84da0 ebp=00b84db4 iopl=0         nv up ei pl nz na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000206
wwlib!DllGetClassObject+0x57ced:
69e87ff8 0fbf5602        movsx   edx,word ptr [esi+2]     ds:002b:1b20d482=8002
0:000> p
eax=00b84dfc ebx=00000001 ecx=00007ff8 edx=ffff8002 esi=1b20d480 edi=00008002
eip=69e87ffc esp=00b84da0 ebp=00b84db4 iopl=0         nv up ei pl nz na pe nc
cs=0023  ss=002b  ds=002b  es=002b  fs=0053  gs=002b             efl=00000206
wwlib!DllGetClassObject+0x57cf1:
69e87ffc 8d1451          lea     edx,[ecx+edx*2]
```

通过调试过程可以看出，当被传送的值为 0x7ff8 时，高 4 字节被扩展为 0x0000，即读取后 edx 的值变成了 0x00007fff8，当被传送的值为 0x8002 时，高 4 字节被扩展为 0xffff，即读取后 edx 的值变成了 0xffff8002，变成了一个负数，导致后续 mov 指令在写入时产生了越界

```
*** writing 0x4e4 to 0x1a064f90 [0x1a034fd0+0x17fde*2+4] (div 3: 0x7ff4)
*** edx will become: 0x17fdf (from 0x7fef+0x7ff8*2)
*** writing 0x4e4 to 0x1a064f92 [0x1a034fd0+0x17fdf*2+4] (div 3: 0x7ff5)
*** edx will become: 0x17fe0 (from 0x7ff0+0x7ff8*2)
*** writing 0x4e4 to 0x1a064f94 [0x1a034fd0+0x17fe0*2+4] (div 3: 0x7ff5)
*** edx will become: 0x17fe1 (from 0x7ff1+0x7ff8*2)
*** writing 0x4e4 to 0x1a064f96 [0x1a034fd0+0x17fe1*2+4] (div 3: 0x7ff5)
*** edx will become: 0x17fe2 (from 0x7ff2+0x7ff8*2)
*** writing 0x4e4 to 0x1a064f98 [0x1a034fd0+0x17fe2*2+4] (div 3: 0x7ff6)
*** edx will become: 0x17fe3 (from 0x7ff3+0x7ff8*2)
*** writing 0x4e4 to 0x1a064f9a [0x1a034fd0+0x17fe3*2+4] (div 3: 0x7ff6)
*** edx will become: 0x17fe4 (from 0x7ff4+0x7ff8*2)
*** writing 0x4e4 to 0x1a064f9c [0x1a034fd0+0x17fe4*2+4] (div 3: 0x7ff6)
*** edx will become: 0x17fe5 (from 0x7ff5+0x7ff8*2)
*** writing 0x4e4 to 0x1a064f9e [0x1a034fd0+0x17fe5*2+4] (div 3: 0x7ff7)
*** edx will become: 0x17fe6 (from 0x7ff6+0x7ff8*2)
*** writing 0x4e4 to 0x1a064fa0 [0x1a034fd0+0x17fe6*2+4] (div 3: 0x7ff7)
*** edx will become: 0x17fe7 (from 0x7ff7+0x7ff8*2)
*** writing 0x4e4 to 0x1a064fa2 [0x1a034fd0+0x17fe7*2+4] (div 3: 0x7ff7)
*** edx will become: 0xffff7ffc (from 0x7ff8+0xffff8002*2)
*** writing 0x4e4 to 0x1a024fcc [0x1a034fd0+0xffff7ffc*2+4] (div 3: 0xffffd554)
```

影响范围:

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

修复方案：

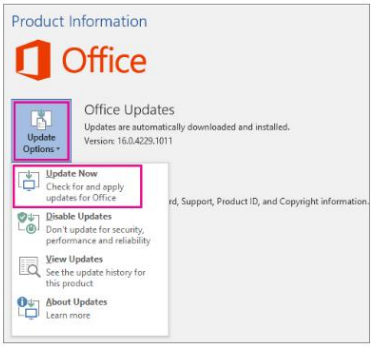
- 安装 Windows Update 2023 年 2 月安全更新
- 或通过 Office 自带入口进行更新

较新版本 | Office 2013 | Office 2010 | Office 2007 | Office 2003

较新版本的 Office

1. 打开任何 Office 应用（如 Word）并创建新文档。
2. 如果已**打开>帐户 (**，请转到**Office**帐户"或"Outlook) "。
3. 在"**产品信息**"下，选择"**更新选项**">"**立即更新**"。

注意: 如果不能立即看到"**立即更新**"选项，可能需要先单击"**启用更新**"。



4. Office 完成检查和安装更新后，关闭"**已是最新版本!**"窗口。

Microsoft Store 中的 Office

如果在设备上从 Microsoft Store 应用Windows Office，Office同一位置更新 Office！

1. 退出所有 Office 应用。
2. 在任务栏搜索中键入"Microsoft Store"并按 **Enter**，打开 **Microsoft Store** 应用。
3. 单击 图标，确保已登录到与你的许可证关联的 Microsoft Office帐户。
4. 单击" "图标> **"下载和更新"**。
5. 单击"**获取更新**"。

注意: 如果单击"**获取更新**"后收到消息"可以正常使用"，则表示无需安装任何新的更新。

- 如果没有在线更新条件，单独下载安装对应版本补丁包
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716

Product	Platform	Impact	Max Severity	Article	Download	Build Number	Details
Microsoft Office 2019 for 32-bit editions	-	Remote Code Execution	Critical	Click to Run	Security Update	https://aka.ms/OfficeS	CVE-2023-21716
Microsoft Office 2019 for 64-bit editions	-	Remote Code Execution	Critical	Click to Run	Security Update	https://aka.ms/OfficeS	CVE-2023-21716
Microsoft Word 2013 Service Pack 1 (64-bit editions)	-	Remote Code Execution	Critical	5002316	Security Update	15.0.5529.1000	CVE-2023-21716
Microsoft Word 2013 RT Service Pack 1	-	Remote Code Execution	Critical	5002316	Security Update	15.0.5529.1000	CVE-2023-21716
Microsoft Word 2013 Service Pack 1 (32-bit editions)	-	Remote Code Execution	Critical	5002316	Security Update	15.0.5529.1000	CVE-2023-21716
Microsoft SharePoint Foundation 2013 Service Pack 1	-	Remote Code Execution	Critical	5002347 5002312	Security Update Security Update	15.0.5529.1000 15.0.5529.1000	CVE-2023-21716
Microsoft Office Web Apps Server 2013 Service Pack 1	-	Remote Code Execution	Critical	5002313	Security Update	15.0.5529.1000	CVE-2023-21716
Microsoft Word 2016 (32-bit edition)	-	Remote Code Execution	Critical	5002323	Security Update	16.0.5383.1000	CVE-2023-21716
Microsoft Word 2016 (64-bit edition)	-	Remote Code Execution	Critical	5002323	Security Update	16.0.5383.1000	CVE-2023-21716

缓解方案：

- 以下两种方式可免受打开未知或不受信任来源的 RTF 文件影响
- 注意缓解方案会影响邮件和文档的图文显示效果

1) Microsoft Outlook 以纯文本方式阅读电子邮件

2) 使用 Microsoft Office 文件阻止策略

该操作需要修改注册表，有一定风险，请提前备份注册表

如需恢复设置

对于 Office 2013

1. 以管理员身份运行 regedit.exe并导航到以下子项:

```
`[HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Security\FileBlock]`
```

2. 将 RtfFiles DWORD 值设置为 0。
3. 将"打开在受保护的视图"DWORD 值设置为 0。

对于 Office 2016

1. 以管理员身份运行 regedit.exe并导航到以下子项:

```
`[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security\FileBlock]`
```

2. 将 **RtfFiles** DWORD 值设置为 **0**。
3. 将 OpenInProtectedView DWORD 值设置为 **0**。

对于 Office 2019

1. 以管理员身份运行 regedit.exe并导航到以下子项:

```
`[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security\FileBlock]`
```

2. 将 **RtfFiles** DWORD 值设置为 **0**。
3. 将 OpenInProtectedView DWORD 值设置为 **0**。

对于 Office 2021

1. 以管理员身份运行 regedit.exe并导航到以下子项:

```
`[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Security\FileBlock]`
```

2. 将 **RtfFiles** DWORD 值设置为 **0**。
3. 将 OpenInProtectedView DWORD 值设置为 **0**。

附录:

- MSRC 官方通告
  https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716