GeekCon

SOLO FREE

办公文档中的隐藏威胁

wh1tc @ Sangfor k team

目录

- OLE功能简介
- 漏洞模式
- 漏洞挖掘
- 漏洞利用
- 漏洞缓解与防御
- Demo

01

OLE功能

简介：简单介绍OLE机制在Office中对应的功能和工作原理

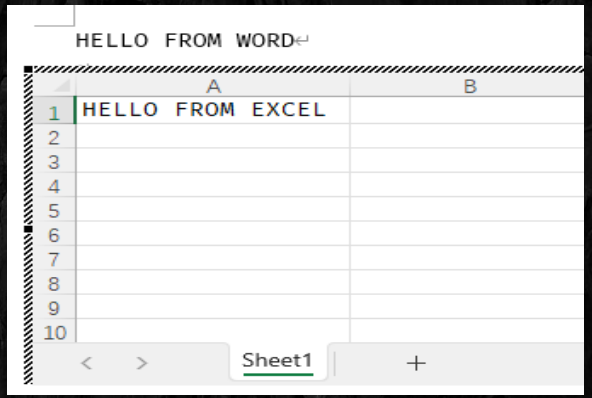
OLE功能

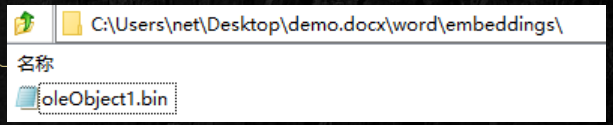
全称：Object Linking and Embedding

在Office中，该组件被用于“对象”功能。

通过“对象”功能，用户可以在单个文档内编辑其他应用程序的相关内容。

以docx格式为例子，“对象”以二进制形式存储在embedding\oleobject1.bin中





工作原理

1. 从文档中获取对应的CLSID

CLSID： 对象的标识符

2. 根据CLSID调用CoCreateInstance来加载对应的对象

3. 如果加载的对象是OLE对象，则进一步调用IpersistStorage

02

漏洞模式

简介：OLE功能对应的安全风险和漏洞模式

漏洞模式

GeekCon

OLE的工作流程中其实存在着一些安全隐患：

1. 文档中的CLSID字段是可以被攻击者控制的
   - CLSID 是不可信的
2. CLSID对应的对象不一定是OLE对象
   - 系统中一般有6000+CLSID，而其中只有200+是OLE对象
3. Office需要先加载CLSID所对应的对象，才能判断这是不是OLE对象
   - 设计缺陷?
   - 很多CLSID对应的对象在设计时没考虑过会被Office加载

漏洞模式

- 在Office加载CLISD所对应的对象的过程中，存在很多安全问题。而其中一个比较严重的安全问题是：“LoadLibrary“函数的错误使用。
  - 比如： HMODULE handle = LoadLibrary("schannel.dll");
- 这里存在一个风险：如果对应的dll文件不存在，应用会从当前工作目录加载对应的dll文件：
  - 而当前工作目录是存在风险的，在特定情况下可以被攻击者预测

03

漏洞挖掘

简介：如何自动化挖掘这类漏洞

漏洞挖掘

GeekCon

自动化思路： 让Office去加载所有的CLISD所对应的对象

1. 收集所有的CLSID
   - 可以写脚本从注册表中提取
   - 也可以使用James Forshaw开发的工具Oleviewdotnet
2. 选择一个用于加载CLSID的文档模板
   - 我们参考了Tavis Ormandy在ProjectZero Issue514使用的模板
   - 使用了RTF中的“clsid” RTF控制字来加载对应的CLSID

漏洞挖掘

GeekCon

3. 使用一个“测试”框架来进行自动化测试

- 生成用于加载特定CLSID的RTF文件
- 自动打开和关闭 该RTF文件

4. 使用微软提供的Process Monitor工具来监控文件系统

- 过滤器设置：
  - Winword.exe 在 测试目录 中 尝试加载不存在的DLL

挖掘结果

在这漏洞模式下，我们发现了两个安全漏洞：

1. CVE-2023-35343 Windows Geolocation 服务远程代码执行漏洞
   - 修复于： 2023年7月11日
   - 影响版本：（补丁前）默认配置下的Windows Server 2022 & 2019
2. CVE-2023-36898 Tablet Windows 用户界面应用程序核心远程代码执行漏洞
   - 修复于： 2023年8月8日
   - 影响版本：（补丁前）默认配置下的Windows 11 21H2 & 22H2

漏洞分析

我们以CVE-2023-35343为例进行漏洞分析：

- 漏洞原因：
  - Office调用CoCreateInstance方法来进行加载对应组件的CLSID
  - 加载组件的时候会调用函数GetFindMyDeviceEnabled
  - 在函数中调用了：`LoadLibraryW(L"mdmcommon.dll")`
  - 而“mdmcommon.dll” 默认配置下没有安装在Windows Server中
- 漏洞效果：
  - 如果当前工作目录中存在恶意的mdmcommon.dll, 就能实现 Office RCE

04

漏洞利用

简介：如何利用这类漏洞

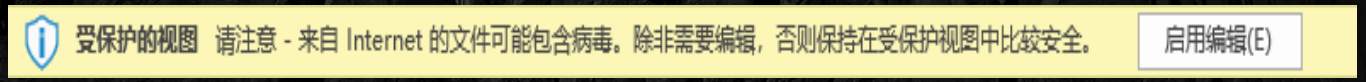
利用条件

这类漏洞原理简单，但是实际利用中需要解决几个问题：

1. 受保护的视图：原理与缺陷
2. 减少需要的用户交互： 选择目标应用和格式
3. 如何进行投递：让恶意DLL文件存在于当前工作目录

受保护的视图

- Office三大应用（Word\Excel\PPT）在打开互联网中下载的文档时，默认会启动受保护的视图。
  - 点击“启用编辑”会 退出受保护的视图



- 在受保护的视图中，会禁用能带来安全危害或者潜在风险的功能：
  - ActiveX / OLE / 宏 / 外部资源加载
- 在一些场景下，受保护的视图不会开启：
  - 没有带有Mark of the Web标签的文档 （从某社交软件中获取的文件）

选择目标应用

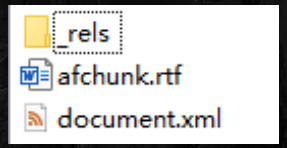
GeekCon

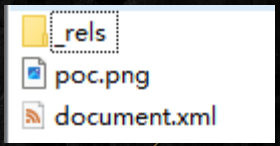
- 为了提高利用的成功率， 我们需要尽可能的减少用户交互
- 对三类支持OLE的应用进行比较

应用程序	简介	受保护的视图	用户交互	补充说明
Office Word 	Office中的文字处理器	支持	打开文档 多次点击	部分格式可减少点击 RTF格式存在缓解
写字板 	Windows默认的文字处理器	不支持 	打开文档 1click	未来将退出系统支持
Office Pub 	Office冷门应用	不支持 	打开文档 1click	部分版本存在缓解

选择目标格式

- Office Word有着更多的用户群体, 攻击者还是会针对该应用。
- 攻击者往往会采用RTF格式进行利用：
  - 优点： 打开文档就触发OLE加载（1click），而DOC/DOCX需要点击OLE对象
  - 缺点： 现实场景中，用户使用RTF格式比较少，容易被警惕
- 为了增加隐蔽性，攻击者现在会伪装成docx格式：
  - CVE-2023-36884在野样本：通过使用 <altChunk> 将RTF嵌在 docx中
  - 可以通过设置docx中的[Content_Types].xml 伪装成任意后缀：
    - <Default Extension="png" ContentType="application/rtf" />





投递

- 漏洞能够完成利用需要：在当前工作目录中加载恶意的DLL
- 根据这一前提：我们可以进行两种方式进行投递：
- ZIP：将恶意文档与恶意DLL一起打包投递。
  - 对DLL的文件属性设置为隐藏，默认设置下用户只能看到恶意docx文档
  - 通过某社交软件投递 或者 利用解压软件的缺陷，可以避免触发保护视图
- WEBDAV：在远程目录下放置恶意文档和恶意DLL
  - 通过修改PROPFIND方法，可以让用户只看得到恶意文档
  - 在钓鱼网站中触发ms-search协议诱导用户点击远程目录下的远程文档

05

漏洞防御

简介：微软的缓解措施以及防御

缓解措施

- 微软对Office进行了一些优化，稍微缓解了这类漏洞的触发。
- 具体措施：
  - .RTF格式：禁止用“oleclsid”控制字 加载CLSID
  - .Pub格式：加载CLSID前会对用户进行安全弹窗警告
- 适用版本：
  - Office 365 当前通道 & 2021/2019/2016 个人版
- 不适用于：
  - Office LTSC 2021/2019 批量激活版 & Office 365 半年更新通道2208版本

防御建议

- 对于个人而言：
  - 使用当前通道的Office版本，其他通道的版本会推迟缓解措施的应用。
  - 及时更新系统版本
  - 警惕来路不明的文档
- 对于安全厂商：
  - 静态扫描： 可以针对特定的CLSID进行检测
  - 热补丁：
    - 针对特定的漏洞：LoadLibrary -> LoadLibraryExW
    - 针对特定的进程：在搜索DLL 的时候移除当前工作目录

06

DEMO

简介：DEMO演示

GeekCon

SOLO FREE

THANKS

日期：10.24