cve-2018-8495-Microsoft Edge 远程命令执行-分析

secular / 2018-10-12 09:16:23 / 浏览数 21185 安全技术 漏洞分析 顶(1) 踩(2)

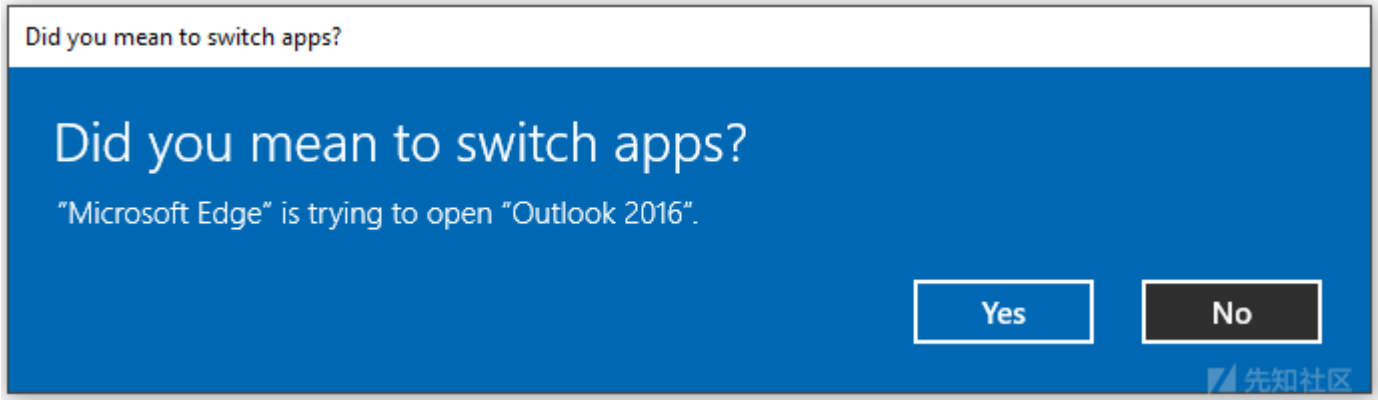
翻译自 https://leucosite.com/Microsoft-Edge-RCE/

漏洞原因

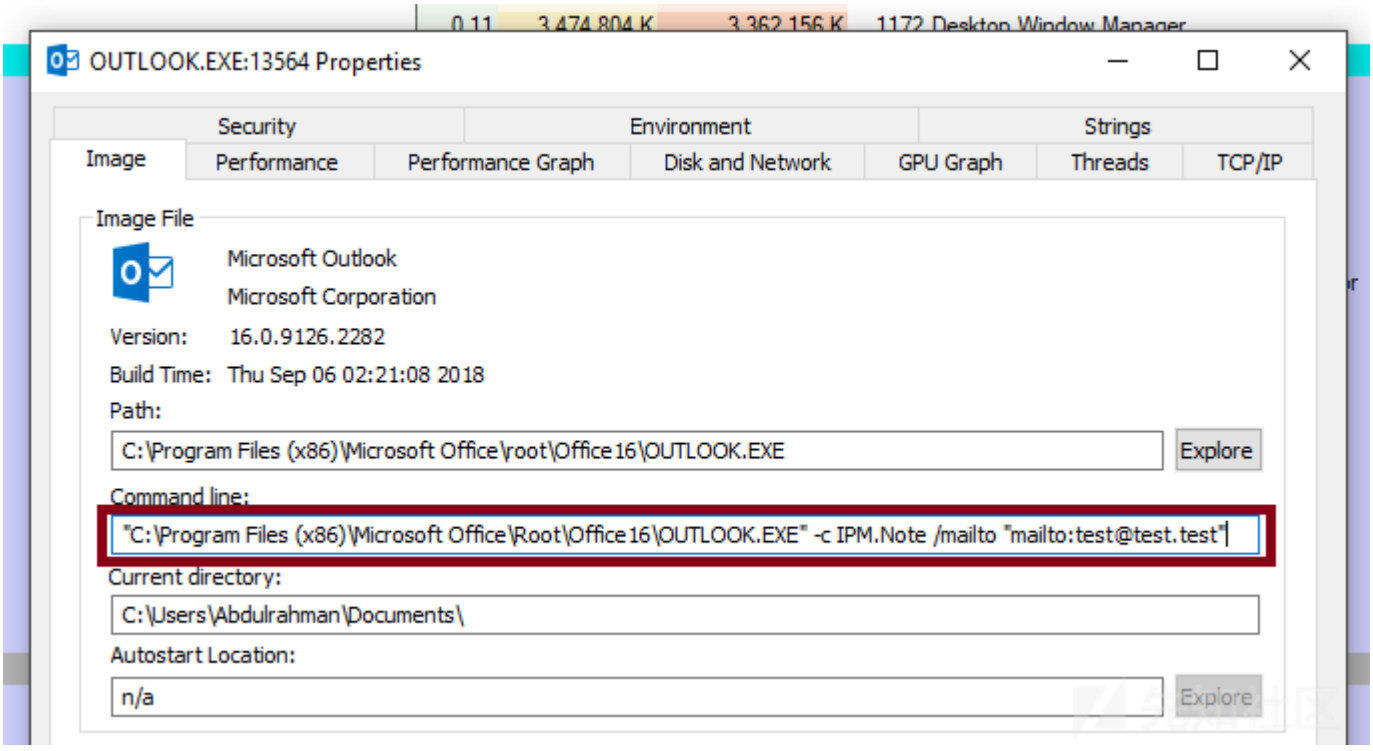
（CVE-2018-8495）漏洞原因主要edge是滥用自定义URI方案，参数过滤存在问题从而实现了远程代码执行。

启动外部应用程序

我们都知道，在浏览器中，可以通过类似这样的'mailto:test@test.test' url来启动默认邮件客户端。
将出现一个提示，询问用户是否切换应用程序，一旦用户同意，应用程序将运行。



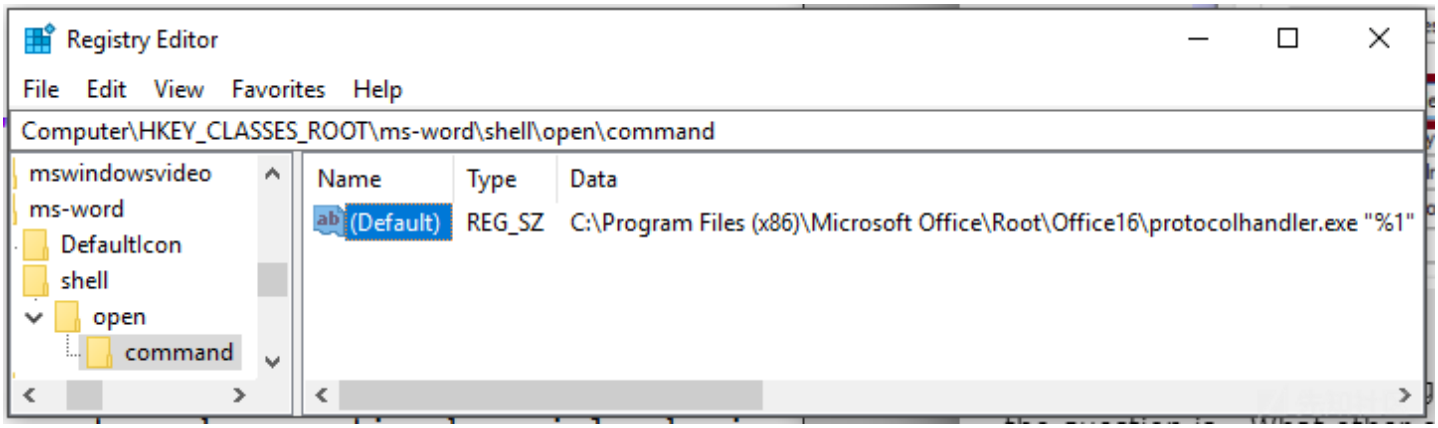
在进行测试中，Outlook是默认的邮件应用程序，如下图所示，某些参数将发送到Outlook。



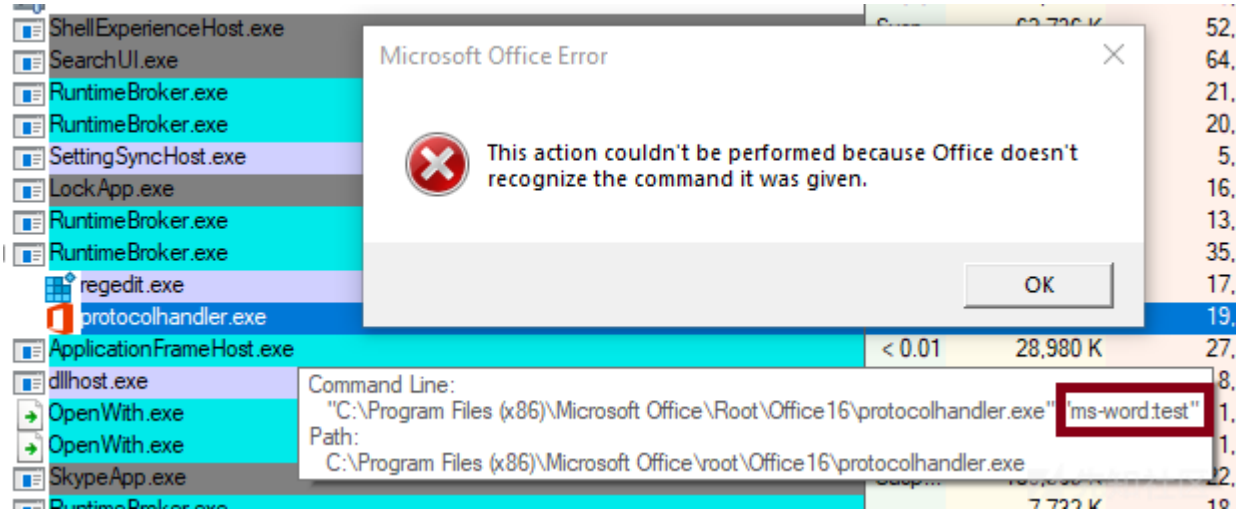
所以，有用户控制的字符串作为参数值传递，显然这里可能会出现问题。但问题是 - 还有哪些外部应用程序启动URI方案？

便捷协议

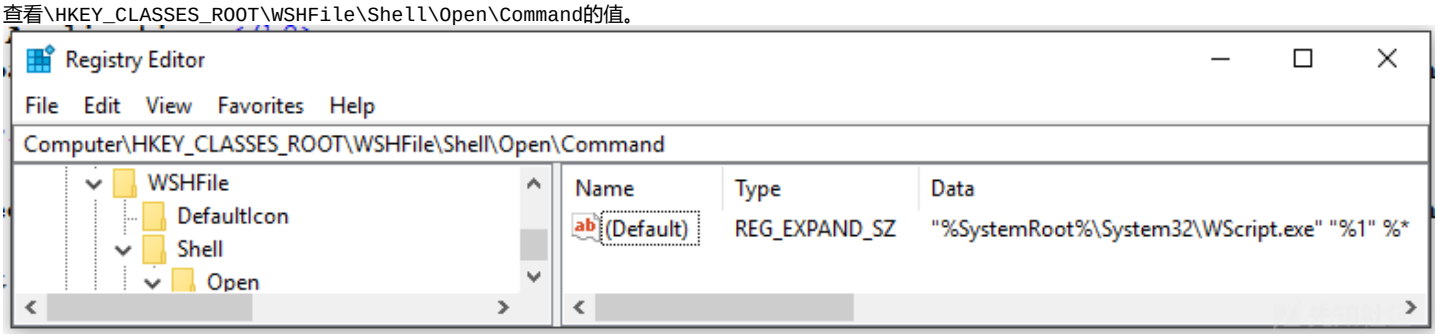
查看注册表时，我们可以找到所有可以使用的注册自定义协议。在注册表Computer\HKEY_CLASSES_ROOT\内部寻找包含shell\open\command子文件夹的子项。例如，



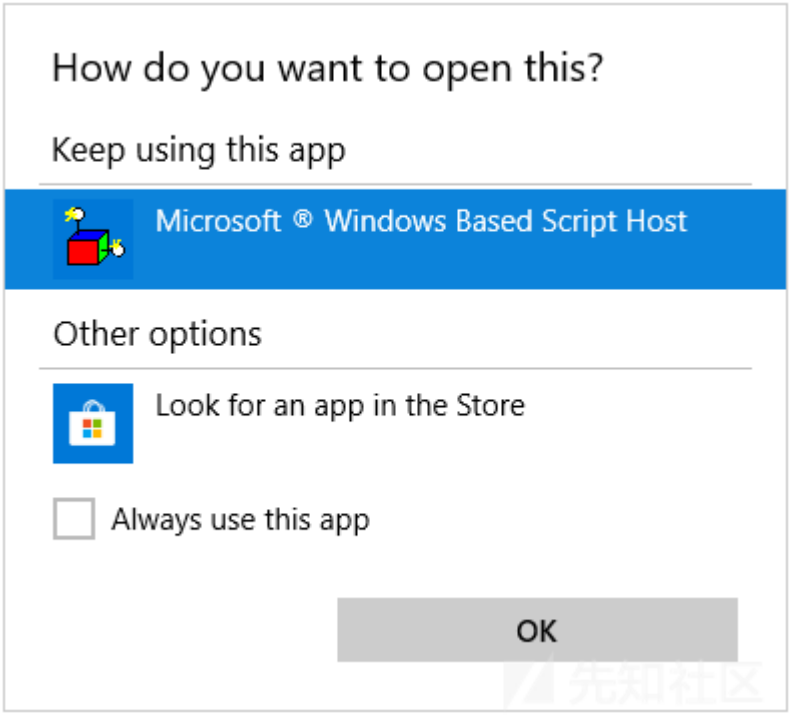
所以，如果我们看看'Computer\HKEY_CLASSES_ROOT\ms-word\shell\open\command'这个注册表项的值，发现是'C:\Program Files (x86)\Microsoft Office\Root\Office16\protocolhandler.exe "%1"'。%1[redacted],这意味着如果我们有一个用户点击一个url标记，指向'ms-word:test'
会发生以下的情况。



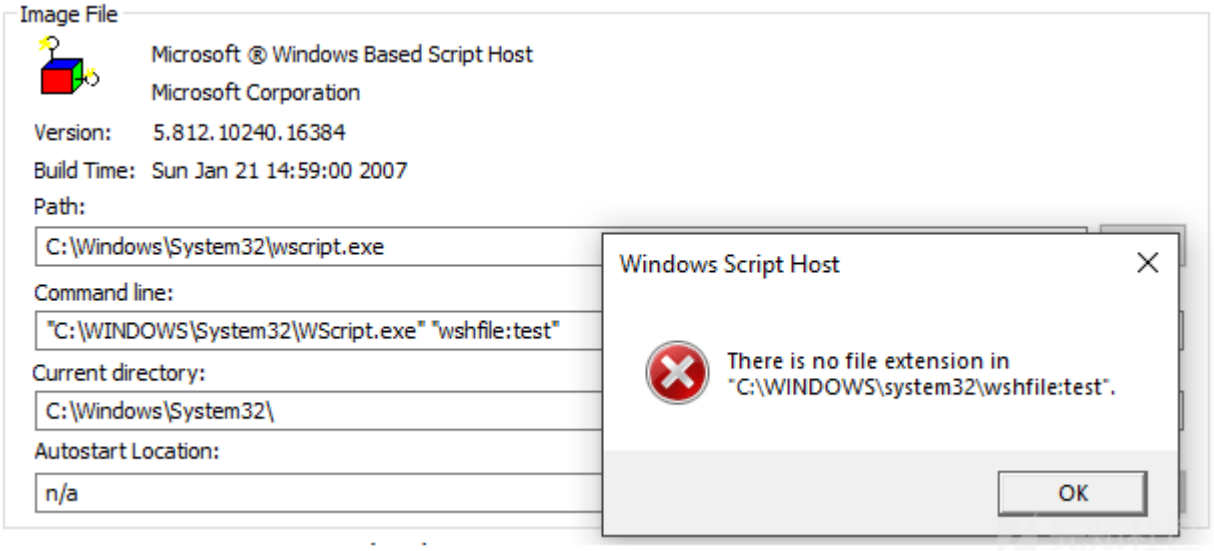
作者没有花时间去查看我们可以抛出的所有可能的命令行参数'protocolhandler.exe'来实现一些有趣的攻击方法。他做了一个简单的尝试。
查看`\HKEY_CLASSES_ROOT\WSHFile\Shell\Open\Command`的值。



嗯，这很方便！一种将用户污染的参数直接传递给的URI方案'WScript.exe'。
"Windows脚本宿主提供了一个环境，用户可以使用各种语言执行脚本，使用各种对象模型来执行任务。"
如果用户 点击url标记'wshfile:test'
从Edge导航会发生什么。首先，我们得到一个提示，要求选择应该处理此URI方案的默认应用程序。默认情况下，正如我们在注册表中看到的那样，'Windows Script Host (WScript.exe)'是处理程序。



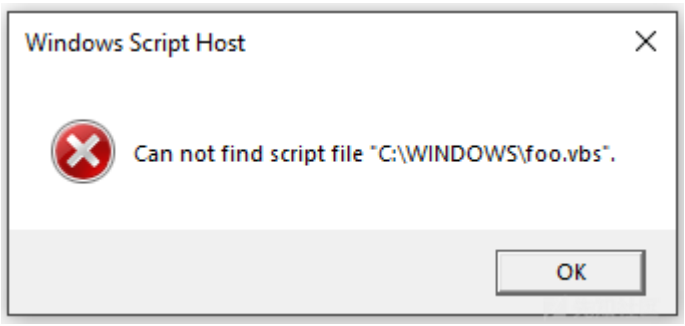
点击 确认后。



'WScript.exe'试图执行位于传递的指定路径的文件。在这种情况下，它试图找到`C:\WINDOWS\system32\wshfile:test`
但它不存在。那么我们能做些什么呢？我们可以以某种方式创建一个名为的文件`wshfile:test`吗？不。所以，我们能做些什么？

漏洞利用

这里的第一个测试思路是显而易见的：路径遍历。我们测试`wshfile:test/../../foo.vbs`， 在提示符下按OK然后：



太棒了！我们现在可以指向任何目录中的任何文件，只要我们可以将文件放在可预测的位置，我们就会有RCE。但说起来容易做起来难，看起来大多数（如果不是所有）来自
Nelson写的一篇很棒的文章的地方。
在本文中，他指出Windows附带了一个签名的VBS'C:\Windows\System32\Printing_Admin_Scripts\en-US\pubprn.vbs'遭受'WSH注入'的困扰。它实质上表明特定的VB
我首先查看了我在Windows中找到的每个VBS文件，然后查看它是否接受任何参数。我发现一个位于

```
'C:\Windows\WinSxS\amd64_microsoft-windows-a..nagement-appvclient_31bf3856ad364e35_10.0.17134.48_none_c60426fea249fc02\SyncApp
```

这个特定的脚本接受一些参数并将它们传递给powershell.exe
shell执行而不过滤它，允许我们注入任意命令。如果你看看'SyncAppvPublishingServer.vbs'的第36行，我们看到：

```
psCmd = “powershell.exe -NonInteractive -WindowStyle Hidden -ExecutionPolicy RemoteSigned -Command■{”■syncCmd■“}”
```

而且我们可以影响它的价值，'syncCmd'但不仅如此，Edge也不会对引号进行过滤，因此我们可以根据需要传递尽可能多的参数'WScript.exe'。同样为了将这个powershell
Hidden'这个参数。
此版本中的问题是此特定文件夹名称取决于用户所在的Windows构建。在我的操作系统版本17134中，该文件夹包含'10
.0.17134'，如果您使用的是其他操作系统，则它将不同。几乎没有关于如何确定这些路径名的信息。
所以，我们所需要的只是Edge中的一个访问漏洞，它允许我们检测本地文件（不读取它们），我无法找到这样的错误。
但是重要的是，我们不必通过猜测整个文件夹名称。在Windows文件夹中有一个名为“DOS PATH”的速记版本，所以猜测文件夹位置的DOS路径版本是可能的。
所以，我们的不需要猜测完整路径。

```
'C:\Windows\WinSxS\amd64_microsoft-windows-a..nagement-appvclient_31bf3856ad364e35_10.0.17134.48_none_c60426fea249fc02\SyncApp
```

只需要使用DOS PATH就可以了

```
'C:\Windows\WinSxS\AMD921~1.48_\SyncAppvPublishingServer.vbs'
```

所以这使我们的攻击更加强大。因为这两个指向完全相同的文件。
至于弹出那个讨厌的提示？没有用户会被愚弄点击“确定”并运行Windows脚本程序的！但是，当出现此提示时，默认焦点位于“确定”按钮上，这意味着用户所要做的就是按

exp

最后的攻击 exp如下

```
<a id="q" href='wshfile:test/../../WinSxS/AMD921~1.48_/SyncAppvPublishingServer.vbs" test test;calc;"'>test</a>
<script>
window.onkeydown=e=>{
   window.onkeydown=z={};
   q.click()
}
</script>
```

具体攻击演示视频如下：
exp

思考

这个漏洞发生在
edge浏览器外部调用过程中，参数没有过滤，同时结合了Windows的便捷协议，以及windows路径变量，思路非常新颖，也表明在复杂的系统中，不同组件之间的调用的

参考链接

1. https://leucosite.com/Microsoft-Edge-RCE/

上一篇：低价手机的隐私泄露问题的相关研究 下一篇：取证分析之逆向服务器提权开启338...

1. 0 条回复
   - 动动手指，沙发就是你的了！