CVE-2019-1388 UAC提权

漏洞描述

CVE-2019-1388 UAC提权是一个Windows证书对话框特权提升漏洞，此漏洞是因为 UAC（用户账户控制）机制的设定不严导致的。默认情况下，Windows UAC 提示本身是由名为 consent.exe 的可执行文件生成的，该可执行文件以 NT AUTHORITY\SYSTEM 身份运行并且有 System 的完整性水平。由于用户可以与此UI 进行交互，因此有必要对 UI 进行严格限制。否则，低特权用户可能能够通过UI操作提权到system权限

漏洞影响

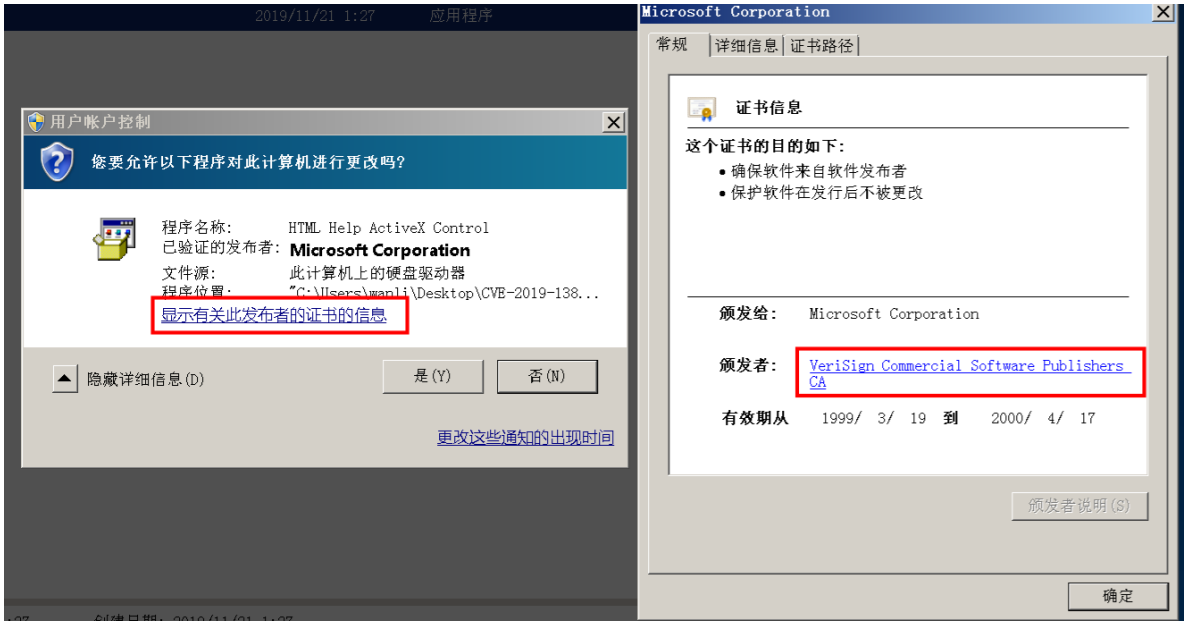
漏洞影响的版本如下

```
windows server机器
Windows 2008r2  7601
Windows 2012r2  9600
Windows 2016    14393
Windows 2019    17763

windows 个人电脑
Windows 7 SP1   7601
Windows 8       9200
Windows 8.1     9600
Windows 10 1511 10240
Windows 10 1607 14393
Windows 10 1703 15063
Windows 10 1709 16299
```

漏洞原理

如果在运行一个可执行文件的时候我们触发了 UAC，在点击「显示有关此发步者的证书的信息」这个链接之后我们可以看到证书里的 Issued by（颁发者） 字段，这个字段对应的值就是 OID值，如果这里是一个超链接就可以提权，如果不是就不行

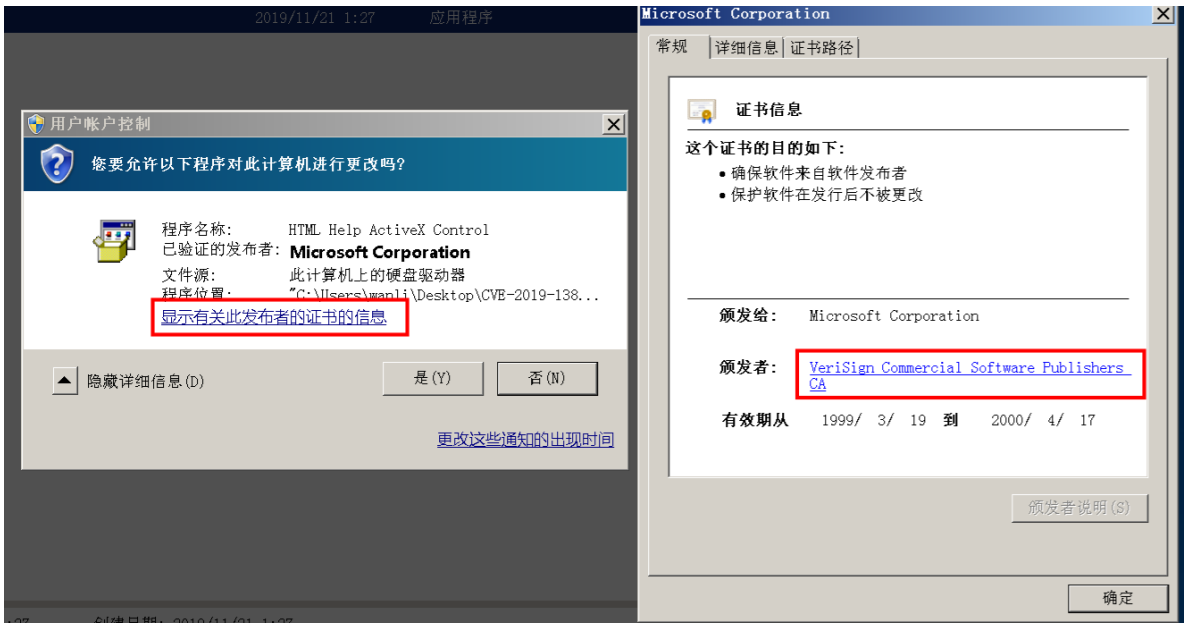


通过点击此链接会触发以 SYSTEM 权限打开浏览器，然后此浏览器就会有 SYSTEM 权限，（浏览器打开必须先要关闭UAC对话框）通过保存按钮打开CMD，CMD就会继承浏览器的 SYSTEM 权限，由此就完成了由普通用户到 NT AUTHORITY\SYSTEM 用户的提权。

漏洞复现

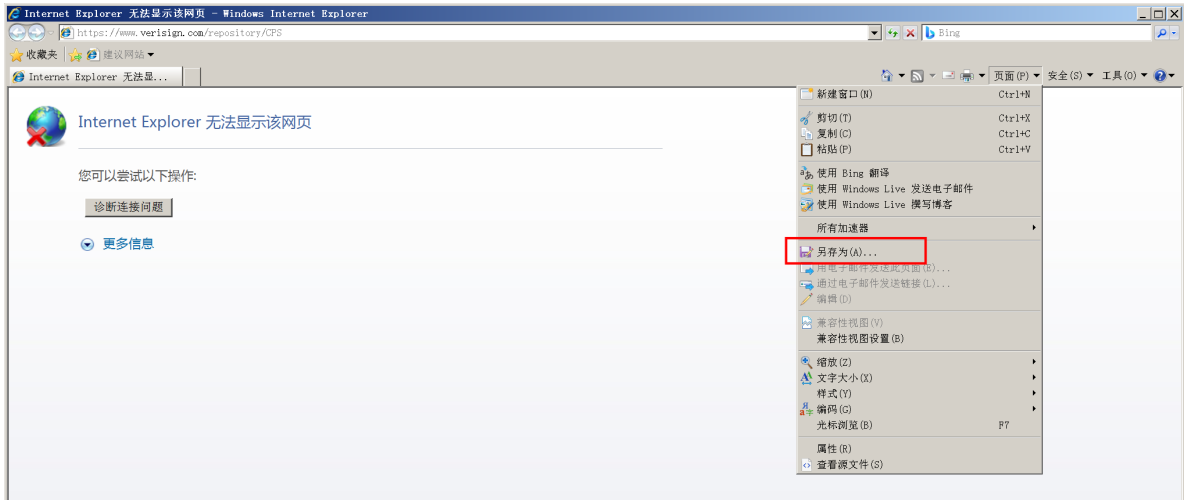
查看当前的用户权限是wanli，是一个低权限

以管理员权限打开HHUPD.EXE，点击显示详细信息里显示的显示有关此发布者的证书的信息

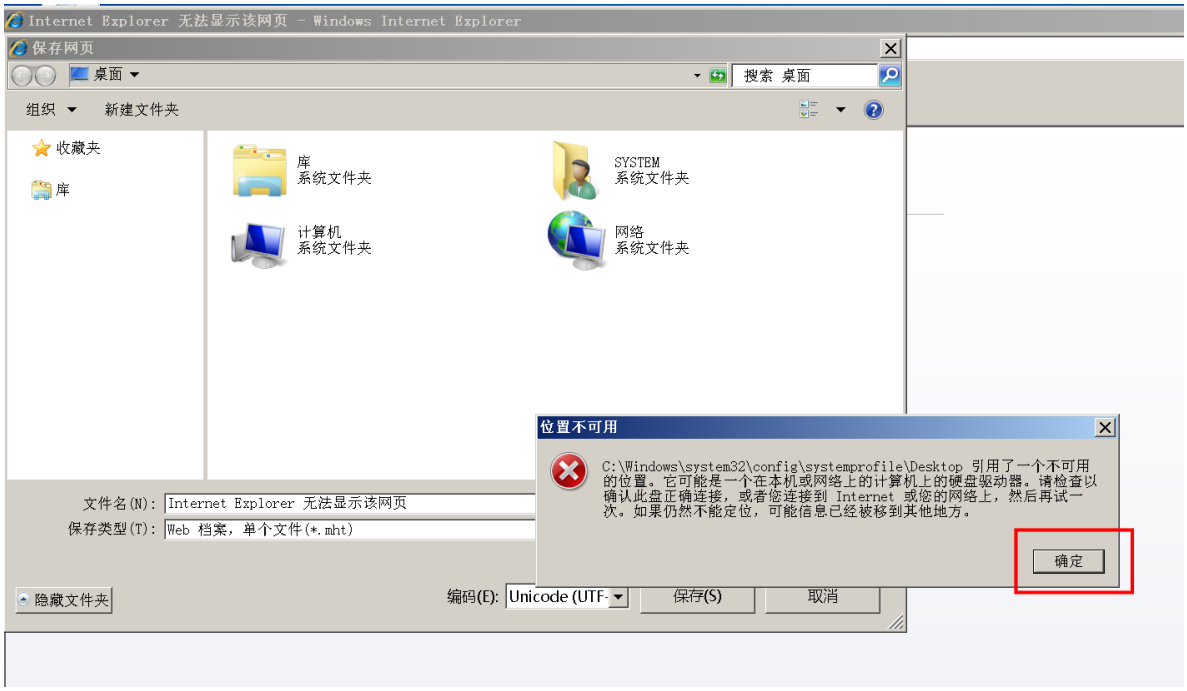


点击该链接之后，关闭上面这两个弹窗，会出现浏览器的页面

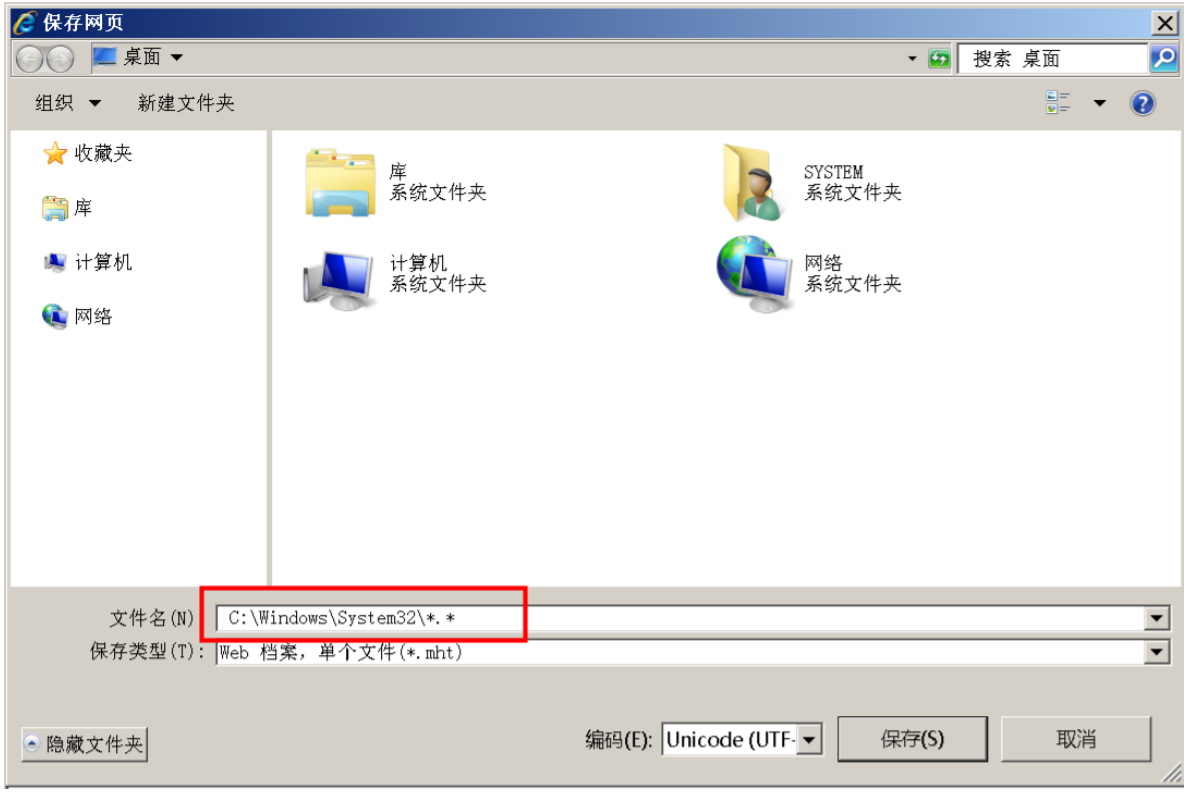
IE浏览器访问链接后点击页面下拉菜单面里的另存为选项



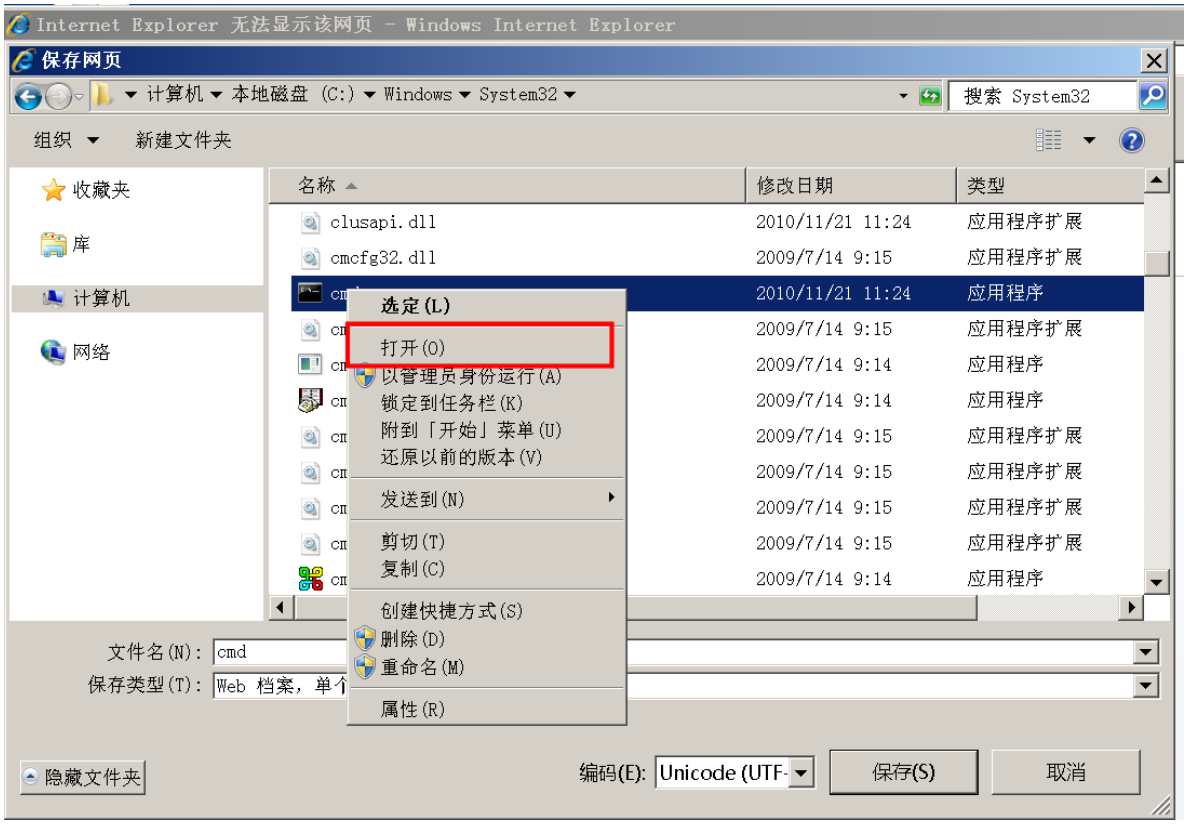
弹出位置不可用的对话框点确定



在文件名的位置输入如下的信息`C:\Windows\System32\*.*`



找到里面的CMD文件，右键打开，即为system权限



查看权限为system