

# Windows UAC 本地权限提升漏洞 (CVE-2019-1388)

## 0x00 漏洞概述:

该漏洞位于 Windows 的 UAC (User Account Control, 用户帐户控制) 机制中默认情况下, Windows 会在一个单独的桌面上显示所有的 UAC 提示 Secure Desktop 这些提示是由名为 `consent.exe` 的可执行文件产生的, 该可执行文件以 `NT AUTHORITY\SYSTEM` 权限运行, 完整性级别为 `System` 因为用户可以与该 UI 交互, 因此对 UI 来说紧限制是必须的, 否则, 低权限的用户可能可以通过 UI 操作的循环路由以 `SYSTEM` 权限执行操作, 即使隔离状态的看似无害的 UI 特征都可能会成为引发任意控制的动作链的第一步。

事实上, UAC 会话中含有尽可能少的点击操作选项, 利用该漏洞很容易就可以提升权限到 `SYSTEM`。

## 0x01 前置条件:

无

## 0x02 影响版本:

服务器版本:

Windows 2008r2 7601  
Windows 2012r2 9600  
Windows 2016 14393  
Windows 2019 17763

PC 版本:

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

## 0x03 环境搭建：

靶机：

Windows 7 专业版 版本 6.1（内部版本 7601：Service Pack 1）

账号：

wql （普通用户权限）

靶机来源：

<https://msdn.itellyou.cn/>

工具：

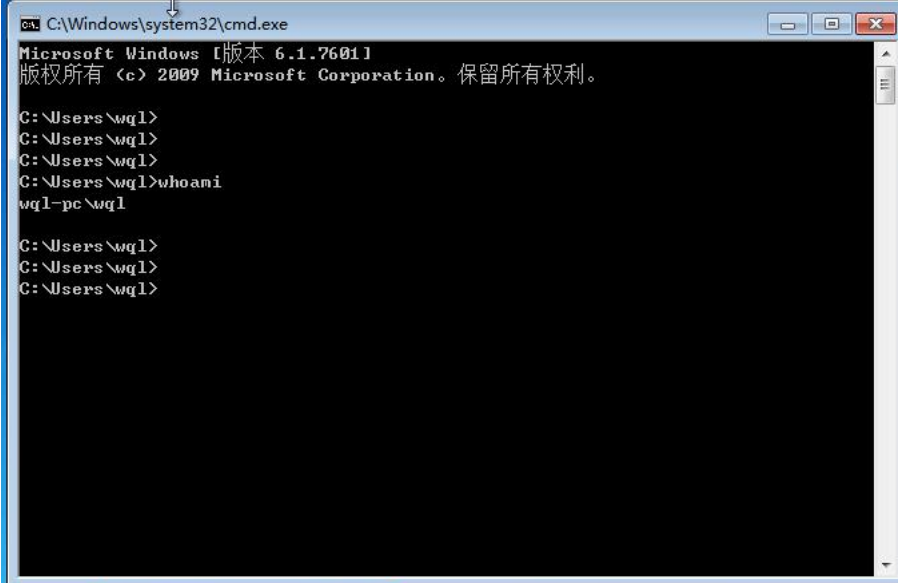
hhupd.exe

工具来源：

<https://github.com/mai-lang-chai/System-Vulnerability/tree/master/Windows/CVE-2019-1388>

## 0x04 漏洞复现：

使用账号 wql 登入系统，win+r 输入 cmd，键入命令 whoami，结果如下，如图 0：



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\wql>
C:\Users\wql>
C:\Users\wql>
C:\Users\wql>whoami
wql-pc\wql

C:\Users\wql>
C:\Users\wql>
C:\Users\wql>
```

图 0

使用管理员权限打开工具 hhupd.exe，点击显示详细信息结果如下，图 1：

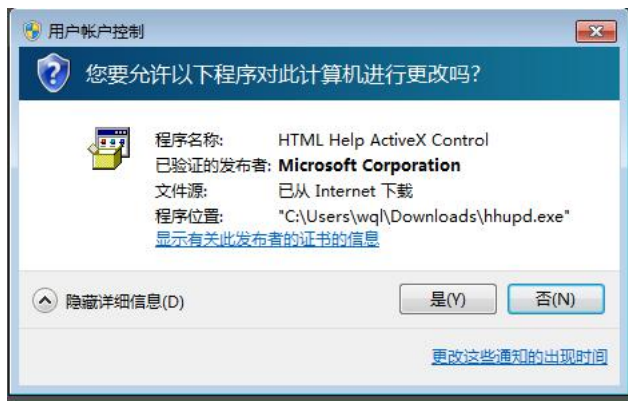


图 1

点击显示有关发布者的证书信息，如下，

图 2:



图 2

点击颁发者，如下，

图 3:

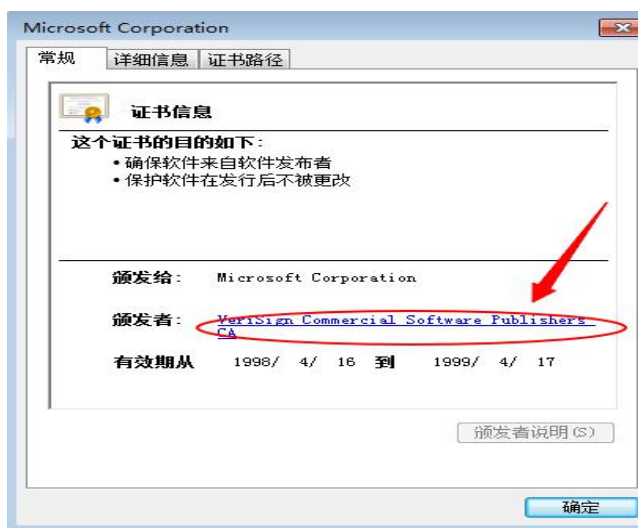


图 3

关闭窗口，这时候浏览器会打开之前点击的链接，（必须要关闭窗口，不然不会显示的），在浏览器中点击页面，另存为，如下，

图 4:

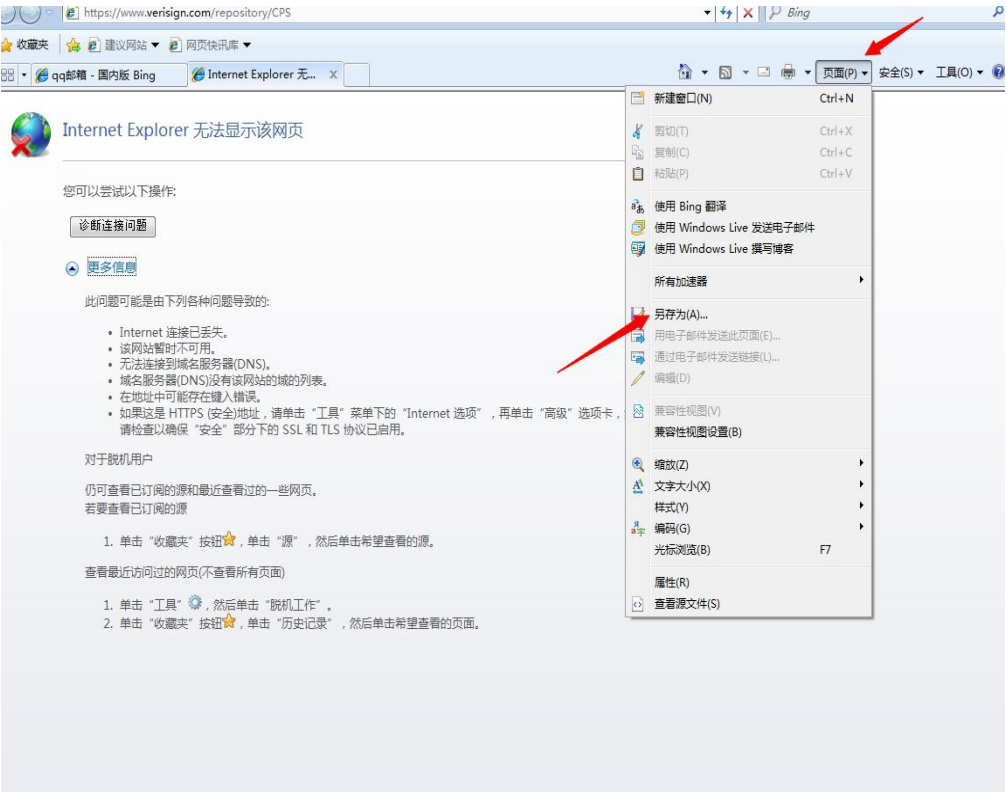


图 4

选择 C:\Windows\System32\cmd ，如下

图 5:

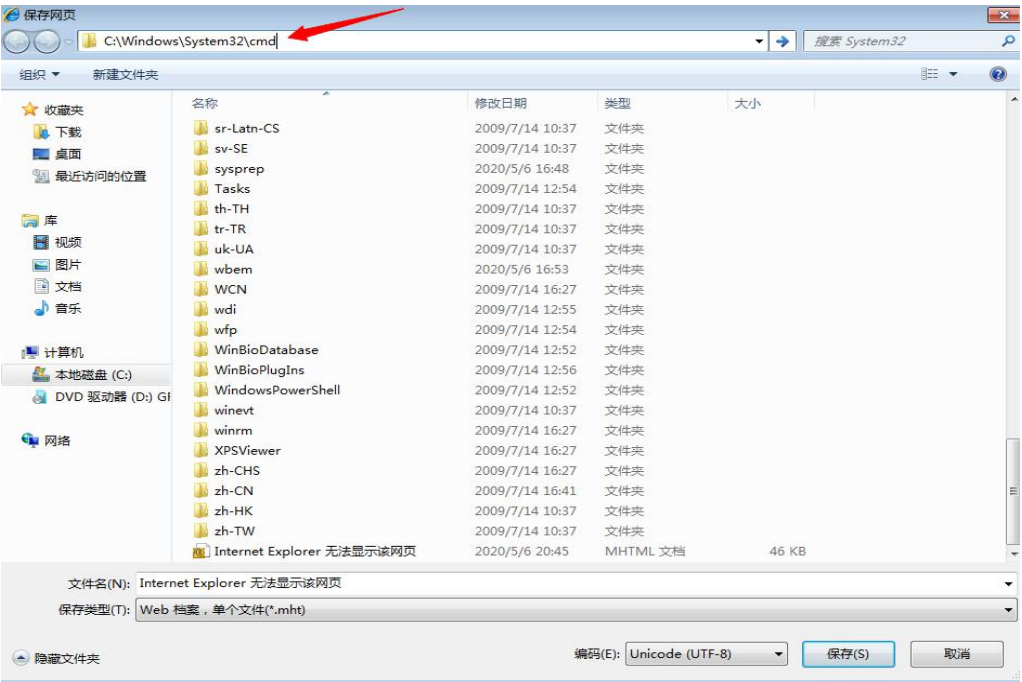


图 5

回车之后就会弹出一个命令提示符窗口，输出命令：whoami  
结果如下图 6：

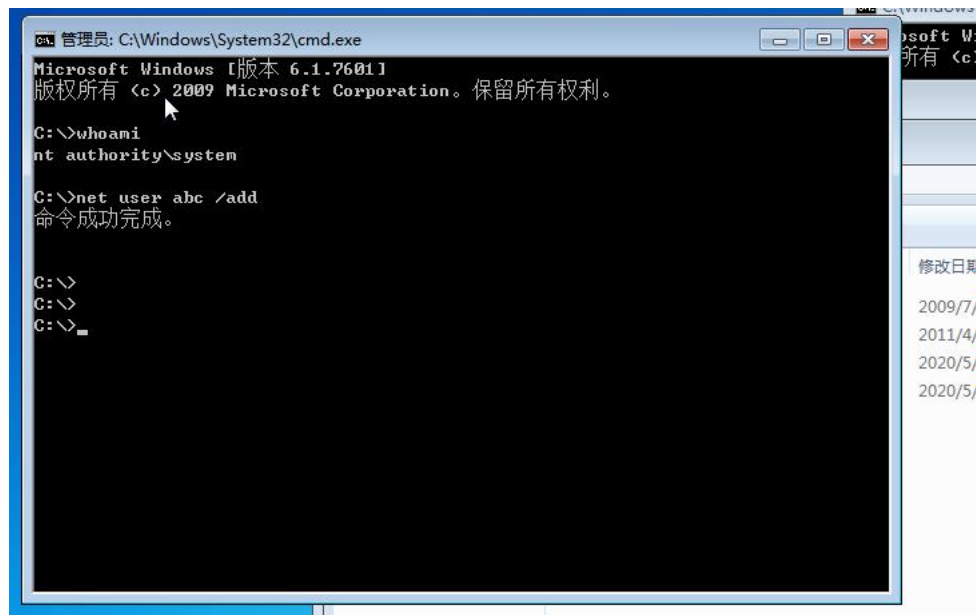


图 6

提权成功。

## 0x05 附录：

有的复现帖子上说 win10 1903 win7 系统都可以，但是实测 win 10 1903 (OS 内部版本 18362.778) 与 win7 (7600)均复现失败。