Windows最新“WebDAV”提权漏洞介绍（MS16-016）

SamSmith 2016-02-15

这个漏洞是由于Windows中的WebDAV未正确处理WebDAV客户端发送的信息导致的。不知各位是否想到了2003年知名的“Microsoft Windows 2000 WebDAV远程缓冲区溢出漏洞”呢？

漏洞CVE编号：CVE-2016-0051。

漏洞信息

据微软安全公告描述：

> 如果 Microsoft Web 分布式创作和版本管理 (WebDAV) 客户端验证输入不当，那么其中就会存在特权提升漏洞。成功利用此漏洞的攻击者可以使用提升的特权执行任意代码。
> 若要利用此漏洞，攻击者首先必须登录系统。然后，攻击者可以运行一个为利用此漏洞而经特殊设计的应用程序，从而控制受影响的系统。
> 工作站和服务器最易受此攻击威胁。此安全更新程序通过更正WebDAV验证输入的方式来修复这个漏洞。

漏洞影响版本

根据微软官方信息显示，此漏洞存在于在：

```
Windows Vista SP2
Windows Server 2008 x86 & x64
Windows Server 2008 R2 x64
Windows 7 x86 & x64
Windows 8.1 x86 & x64
```

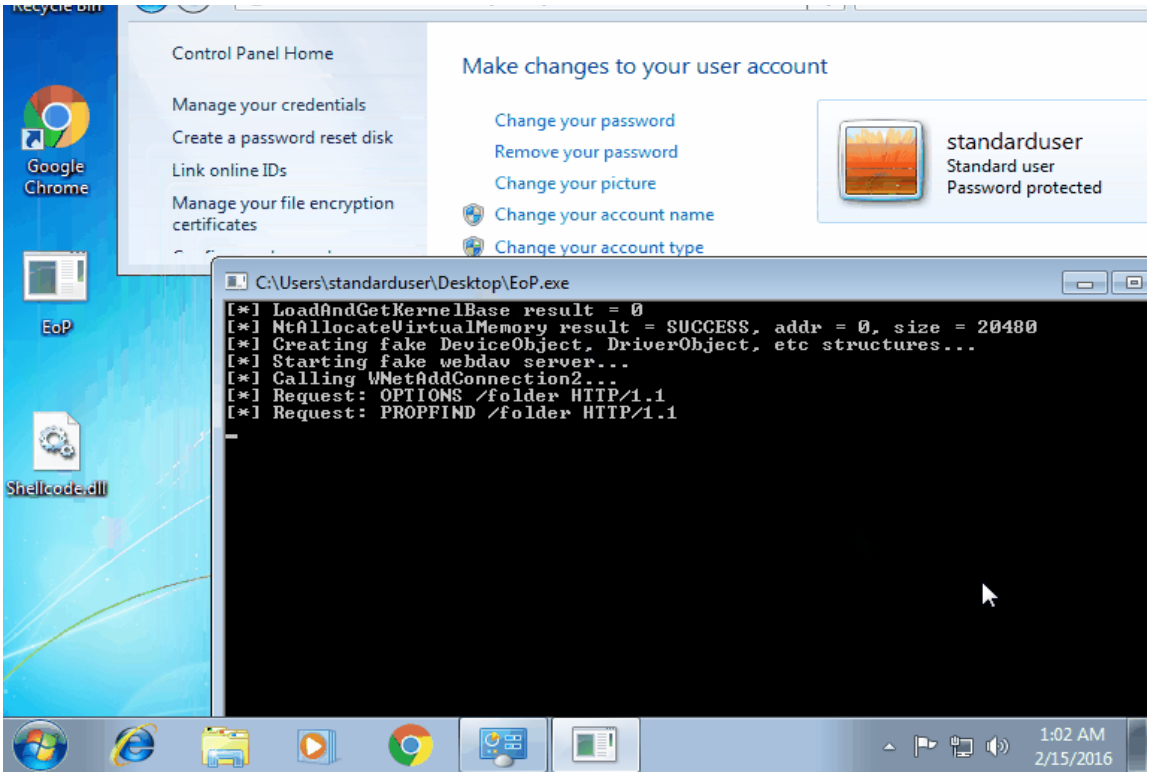
系统中提升权限至系统权限，以下系统中导致系统拒绝服务（蓝屏）：

```
Windows Server 2012
Windows Server 2012 R2
Windows RT 8.1
Windows 10
```

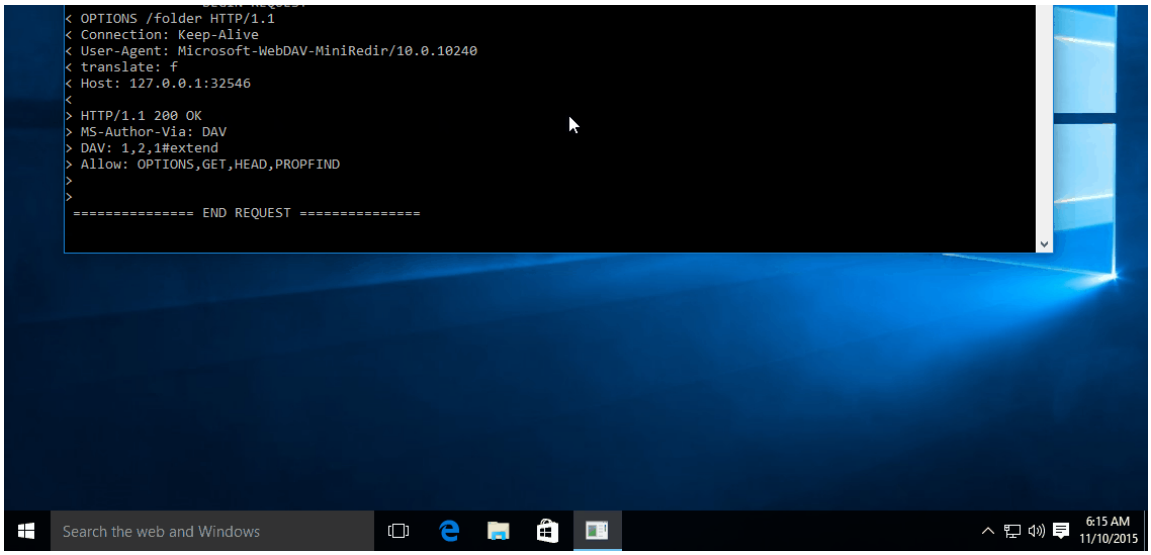
漏洞演示

漏洞作者在GitHub发布了PoC和EXP的演示内容如下。

EXP可在Windows 7 SP1 x86提升权限至系统权限：



PoC 可在Windows 10 x64系统中导致蓝屏：



漏洞发现时间轴

```
2015.9.18 该漏洞被发现
2015.9.24 作者将漏洞以及PoC代码提交至MSRC（微软安全应急响应中心）
2015.9.25 MSRC受理了报告，将相关信息发至分析师进行处理
2015.9.30 MSRC确认该漏洞，将会在补丁中进行修复，并表示了致谢
2016.2.9 漏洞在微软今年发布的二月的“周二补丁日”中被修复
2016.2.9 发布BSoD PoC
2016.2.11 MSRC通知作者他们已经修复了此漏洞
```

2015-08-19

查看全部

小酒馆
公开课
商城
漏洞盒子

登录

必须（保密）

邮箱

请输入邮箱地址

表情 插图

提交评论(Ctrl+Enter) 取消 有人回复时邮件通知我

SamSmith
In this world full of people there's one killing ME
7篇文章 10条评论

关键字查找

相关阅读

- 微软修复Bitlocker驱动器加密工具的…
- 微软公布蓝帽子黑客大赛赛程 赢家得2…
- Windows最新“WebDAV”提权漏洞…
- 微软Windows FastFAT.sys FAT分区拒…
- IE漏洞攻防编年简史

特别推荐

不容错过

一周海外安全事件回顾（2014.03.10-2014.03.16）

blackscreen 2014-03-18

网络小黑揭秘系列之私服牧马人

360天眼实验室 2015-12-01

一周海外安全事件回顾（2014.03.03-2014.03.09）

blackscreen 2014-03-10

外媒称小米、华为、联想等26种手机被预装间谍应用

JackFree 2015-09-04