登录

CVE-2017-0213 Windows COM 特权提升漏洞组件

ly55521 / 2017-06-07 06:41:10 / 浏览数 7430 安全技术 漏洞分析 顶(0) 踩(0)

CVE-2017-0213 Windows COM 特权提升漏洞组件先看看这个漏洞的介绍：

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0213

Windows COM Aggregate Marshaler在实现中存在权限提升漏洞，可使远程攻击者以提升的权限执行任意代码。

白话文：在封装COM组件可提权

微软官方说：

特权提升存在于Windows
COM封装。攻击者成功地利用该漏洞可以运行任意代码具有较高的特权。为了利用该漏洞，攻击者可以运行一个特制的应用程序，可以利用漏洞。此漏洞本身不允许任意代

受影响的版本如下：

<table> Product Version Update Tested Windows 10 √ Windows 10 1511
Windows 10 1607 Windows 10 1703 √ Windows 7 SP1 √ Windows 8.1
Windows RT 8.1 Windows Server 2008 SP2 Windows Server 2008 R2 SP1 Windows Server 2012
Windows Server 2012 R2 Windows Server 2016 </table>

基本存在于比较新的win个人电脑和服务器操作系统了、收藏下利用工具。

https://github.com/WindowsExploits/Exploits

漏洞工具提供者已编译好了 win32和64位的 exe 了

用win64测试下、好用。

点击收藏 | 0 关注 | 0
上一篇：漏洞修复方案汇总Book 下一篇：针对西门子PLC蠕虫的实现
1. 6 条回复


simeon 2017-06-07 07:06:15

好东西。不错！

0 回复Ta

章鱼小团子 2017-06-07 08:14:53

赞，很好用

0 回复Ta

uber 2017-06-08 16:54:28

这个怎么改成指定命令执行模式？
自己编译的时候出现问题如下：

```
1>------ ■■■■■:  ■■: CVE-2017-0213, ■■: Release Win32 ------
1>  CVE-2017-0213.cpp
1>CVE-2017-0213.cpp(376): error C2280: “ScopedHandle::ScopedHandle(ScopedHandle &)”: ■■■■■■■■■■
1>          CVE-2017-0213.cpp(318) : ■■“ScopedHandle::ScopedHandle”■■■
========== ■■:  ■■ 0 ■■■■ 1 ■■■■ 0 ■■■■ 0 ■ ==========
```

定位到代码报错处：

```
ScopedHandle hLink;

NTSTATUS status = pfNtCreateSymbolicLinkObject(hLink.ptr(), SYMBOLIC_LINK_ALL_ACCESS, &objAttr, &target);
if (status == 0)
{
printf("Opened Link %ls -> %ls: %p\n", linkname, targetname, hLink.get());
return hLink;    //■■■■■■
}
else
{
printf("Error creating link %ls: %08X\n", linkname, status);
return ScopedHandle();
}
```

请问此LZ有处理此问题的方法么？

0 回复Ta

 hades 2017-06-09 01:23:31

https://xianzhi.aliyun.com/forum/read/1698.html

朋友给出了加用户版本ing

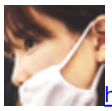
0 回复Ta

 ly55521 2017-06-09 02:51:29

没有，我没装vs、没编译、 你这个可能是 vs 版本问题， http://bbs.csdn.net/topics/391080604 ， 或者修改代码 参考下这里 http://www.it1352.com/540513.html

提权一般都是有了webshell呀，用这个提权后就是系统用户权限了，想执行啥就执行啥。

0 回复Ta

 hades 2017-06-12 01:31:49

感谢支持ing

0 回复Ta

登录 后跟帖

先知社区

现在登录

热门节点

技术文章

社区小黑板

目录

RSS 关于社区 友情链接 社区小黑板