CVE-2017-0213 Windows COM 特权提升漏洞EXP 直接加用户版

castiel / 2017-06-08 01:04:48 / 浏览数 22193 安全工具 工具 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://bugs.chromium.org/p/project-zero/issues/detail?id=1107
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。
受影响的版本如下： Product VersionUpdateTestedWindows 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 2008R2 SP1 Windows Server 2012 Windows Server 2012R2 Windows Server 2016
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。
国外大牛编译的是直接弹CMD的EXP 源码地址：https://github.com/WindowsExploits/Exploits
本想改个命令行版的在webshell环境下用 但发现webshell环境下不能成功 技术有限只改了个直接加用户的exp
运行exp后会在系统中直接加个 admin 的用户 密码：Qwer!@#123

编译环境：Windows7 + VS2013
[attachment=5916]

CVE-2017-0213.rar (11.8 MB) 下载附件

点击收藏 | 0 关注 | 0

上一篇：hashcat-utils密码综合... 下一篇：小米圈SSRF引发思考到富文本XSS

1. 14 条回复

by小白 2017-06-08 02:06:22

已笑纳 感谢分享

0 回复Ta

奶酪只有一块 2017-06-08 07:31:27

感谢分享。

0 回复Ta


all0shell 2017-06-09 14:14:38

谢谢分享!!

0 回复Ta


想飞的菜鸟 2017-06-10 12:58:32

有可执行的吗？ 这个虚拟机测试没成功！ 虚拟机是去年的系统

0 回复Ta


uber 2017-06-10 14:38:19

谢谢分享！
有一个使用问题，windows 10
x64环境，本次开机运行EXP，可以成功添加用户，删除用户后再执行一个EXP，添加用户失败，请问只有我自己出现这个问题么？

0 回复Ta


castiel 2017-06-12 03:20:20

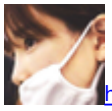
W10上我没测试过 我测试环境是2008的 可能还是跟环境有关吧

0 回复Ta


zone2016 2017-06-19 02:15:41

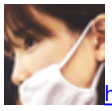
抱歉！页面无法访问……

0 回复Ta


hades 2017-06-19 03:13:40

？？？？

0 回复Ta


hades 2017-06-23 01:25:40

https://github.com/WindowsExploits/Exploits/blob/master/CVE-2017-0213/Source/CVE-2017-0213.cpp

0 回复Ta


我是无名 2017-08-04 00:01:12

谢谢了

0 回复Ta


三叶草 2017-08-11 02:31:59

谢谢分享

0 回复Ta


bloody 2017-08-12 15:05:52

拿走拿走！！！！

0 回复Ta


bini. 2017-08-15 14:04:59

失效了！

0 回复Ta


vaf 2017-08-17 03:23:09

最近刚好在收集~~

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