GhostScript沙箱绕过(命令执行漏洞)CVE-2018-16509

原创

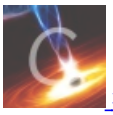
她叫常玉莹 于 2020-07-27 19:39:35 发布 669 收藏

分类专栏： 漏洞复现 文章标签： docker linux 安全 安全漏洞 黑盒测试

版权声明：本文为博主原创文章，遵循 CC 4.0 BY 版权协议，转载请附上原文出处链接和本声明。

本文链接：https://blog.csdn.net/qq_45924653/article/details/107619461

版权



漏洞复现 专栏收录该内容

4 篇文章 0 订阅

订阅专栏

2018年8 月 21 号，Tavis Ormandy 通过公开邮件列表，再次指出 GhostScript 的安全沙箱可以被绕过，通过构造恶意的图片内容，将可以造成命令执行、文件读取、文件删除等漏洞。

GhostScript 被许多图片处理库所使用，如 ImageMagick、Python PIL 等，默认情况下这些库会根据图片的内容将其分发给不同的处理方法，其中就包括 GhostScript。

访问http://192.168.0.104:8080上传poc.png 执行id > /tmp/success && cat /tmp/success

命令docker-compose exec web bash进入容器 ls /tmp/看到success文件已经创建

```
root@clay-virtual-machine:/home/clay/Desktop/vulhub/ghostscript/CVE-2018-16509# docker-compose exec web bash
root@4ce102f27358:/# ls /tmp/
success
root@4ce102f27358:/#
```

使用命令测试该漏洞

```
docker run -it --rm --name im -v `pwd`/poc.png:/poc.png vulhub/imagemagick:7.0.8 c
```

```
root@clay-virtual-machine:/home/clay/Desktop/vulhub/ghostscript/CVE-2018-16509# docker run -it --rm --name im -v
`pwd`/poc.png:/poc.png vulhub/imagemagick:7.0.8 convert /poc.png /poc.gif
uid=0(root) gid=0(root) groups=0(root)
convert: FailedToExecuteCommand `'gs' -sstdout=%stderr -dQUIET -dSAFER -dBATCH -dNOPAUSE -dNOPROMPT -dMaxBitmap=5
00000000 -dAlignToPixels=0 -dGridFitTT=2 '-sDEVICE=pngalpha' -dTextAlphaBits=4 -dGraphicsAlphaBits=4 '-r72x72' -g
612x792  '-sOutputFile=/tmp/magick-1sUjuqEo1OcGG%d' '-f/tmp/magick-1p9Owmaq7NG0E' '-f/tmp/magick-1BnfZjCEg9elD' -
c showpage' (-1) @ error/delegate.c/ExternalDelegateCommand/462.
convert: no images defined `/poc.gif' @ error/convert.c/ConvertImageCommand/3288.
root@clay-virtual-machine:/home/clay/Desktop/vulhub/ghostscript/CVE-2018-16509#
```

id命令已经执行

> 人生漫漫其修远兮，网安无止境。
> 一同前行，加油！