Bash Shellshock CVE-2014-6271破壳漏洞复现

一、Shellshock的背景

Shellshock，又称Bashdoor，是在Unix中广泛使用的Bash shell中的一个安全漏洞，首次于2014年9月24日公开。许多互联网守护进程，如网页服务器，使用bash来处理某些命令，从而允许攻击者在易受攻击的Bash版本上执行任意代码。这可使攻击者在未授权的情况下访问计算机系统。

二、通过试验和总结，Shellshock漏洞执行的条件

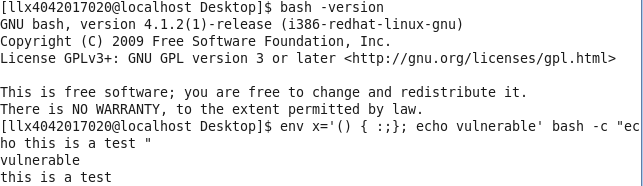
1、首先是Unix、linux等系统下的bash版本必须小于等于4.1版本；

2、可以猜出/cgi-bin/下目录的文件；例如：/cgi-bin/test-cgi、/cgi-bin/test.sh、/cgi-bin/test.py、/cgi-bin/test.perl等等；

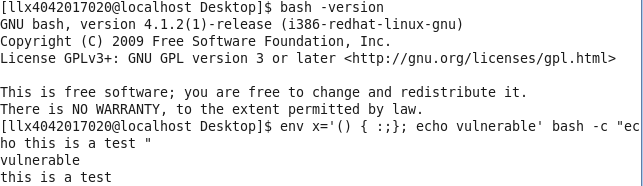
3、/cgi-bin/下的脚本文件通过系统环境变量调用bash的环境

三、漏洞复现

1、检测版本 $ bash -version



2、检测是否存在破壳漏洞 $ env x=’() { :;}; echo vulnerable’ bash -c "echo this is a test ",如果输出vulnerable,并继续打印this is a test则说明存在该漏洞。



四、漏洞分析

漏洞的关键在于bash会把定义的各种函数放到env里面去，大致的格式如下：

$ function foo { echo bar; }

$ export -f foo

$ env | grep -A1 foo

foo=() { echo bar

}

以(){开头的字符串作为环境变量的值来将函数定义导出为环境变量，而bash在处理这样的函数环境变量时没有以}为结束，而时一直执行shell命令，bash会在导处函数处理环境时执行用户代码。

五、漏洞的利用

通过客户端request请求进行header头传参（用户想执行的代码），在header头的任何位置添加你想执行的脚本。