**Shellshock漏洞复现实验报告**

漏洞相关CVE编号 CVE-2014-6271

马志立4042017021

1. 原理分析

ShellShock漏洞出现时间很早，它的的原理是利用了Bash在导入环境变量函数时候的漏洞，启动Bash的时候，它不但会导入这个函数，而且也会把函数定义后面的命令执行。因此一些服务器的bash版本过低，攻击者把有害数据写入环境变量，cgi脚本调用了bash命令后，有害数据会传到服务器端，触发服务器运行Bash脚本，完成攻击。

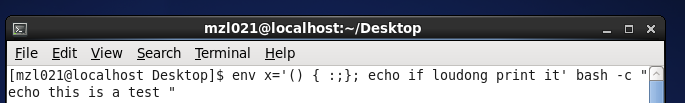
1. 复现准备

虚拟机：CentOS 6

Bash版本：4.1.2

1. 复现过程

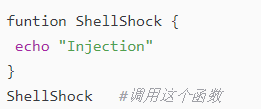
在命令行定义一个echo函数使其输出this is a test,并且在函数后面定义一个命令：if loudong print it（意为如果有漏洞，输出它）



执行后发现，在函数出书“this is a test”之前，还输出了if loudong print it，由此浮现了shellshock漏洞，证明了函数定义后面的命令也会被误执行

1. 原因分析

Bash的自定义函数shellshock为：



环境变量：



bash读取了环境变量，在定义ShellShock之后直接调用了后面的bash命令。

所以一旦调用bash，自定义的语句就直接触发。

1. 修复办法

将虚拟机的bash版本升级到最新即可。