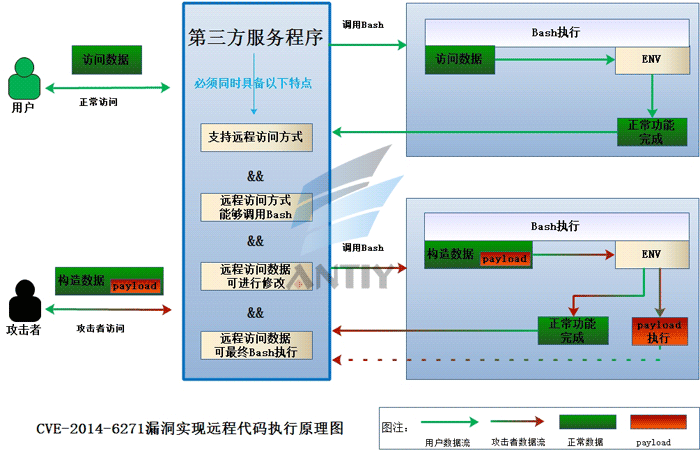
# Bash Shellshock(破壳)漏洞分析

1. 漏洞原理

Bash支持通过进程环境导出shell变量和shell函数到子进程的其他的bash实例中。现有的bash版本使用环境变量实现这一过程。环境变量以函数名命名，以“() { }”作为环境变量的值传送函数定义。由于bash处理函数定义后仍会继续解析和执行跟在函数定义后的shell命令导致远程任意代码执行。

核心原因：没有严格限制输入的边界，没有合法化的参数判断。

从阐述的漏洞原理可知，漏洞的根本原因存在于bash的ENV命令实现上，因此漏洞本身是不能够直接导致远程代码执行的。如果达到远程代码执行的目的，必须要借助第三方服务程序作为媒介才能够实现，第三方服务程序也必须要满足众多条件才可以充当此媒介的角色。例如，第三方服务程序apache2便可充当此媒介，其CGI组件满足远程访问并调用bash的ENV命令进行访问数据解析功能。具体如何实现，见下面的原理图：CVE-2014-6271漏洞实现远程代码执行原理图。

1. 漏洞危害

该漏洞会影响（2014年）主流的Linux和Mac OSX操作系统平台，包括但不限于Redhat、CentOS、Ubuntu、Debian、Fedora、Amazon Linux、OS X 10.10等平台。该漏洞可以通过构造环境变量的值来执行想要执行的攻击代码脚本，会影响到与Bash交互的多种应用，包括HTTP、OpenSSH、DHCP等。根据目前的漏洞验证情况以及已经流传的POC情况，这个漏洞将严重影响网络基础设施的安全，包括但不限于网络设备、网络安全设备、云和大数据中心等。特别是Bash广泛地分布和存在于设备中，其消除过程将非常长尾，且易于利用其编写蠕虫进行自动化传播，同时也将导致僵尸网络的发展。

三．漏洞验证方法

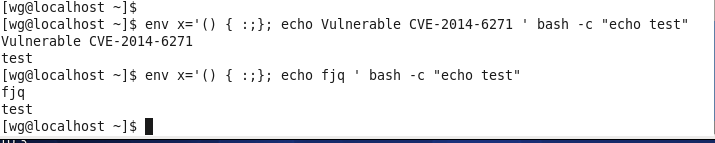
目前的bash脚本是以通过导出环境变量的方式支持自定义函数，也可将自定义的bash函数传递给子相关进程。一般函数体内的代码是不会被执行，但此漏洞会错误的将“{}”花括号外的命令进行执行。

本地验证方法：

在shell中执行下面命令：

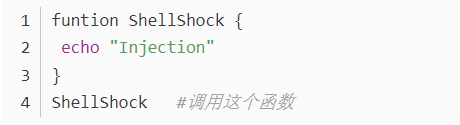
env x='() { :;}; echo Vulnerable CVE-2014-6271 ' bash -c "echo test"

执行命令后，如果显示Vulnerable CVE-2014-6271，证系统存在漏洞，可改变echo Vulnerable CVE-2014-6271为任意命令进行执行。

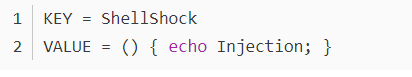


四．漏洞细节分析

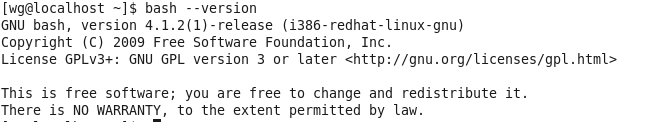
1.了解bash自定义函数，只需要函数名就能够调用该函数。



1. 这个时候的Bash的环境变量：



1. Bash 版本小于等于4.3



1. 什么是shellshock

ShellShock是一个BashShell漏洞(据说不仅仅是Bash，其他shell也可能有这个漏洞).

一般情况来说，系统里面的Shell是有严格的权限控制的，如果没有相应的权限，是根本看不到某些命令的存在，更不要说执行这些命令。

但是，Bash在运行的过程中会调用操作系统的环境变量，并且会执行一些设置命令。通过ShellShock漏洞，入侵者可以把某些”本来没有权限执行的语句或者命令“，注入到环境变量里。当bash设置环境变量的时候，就会执行这些”被注入“命令。这样子便绕过用户权限的限制，把一些”没有权限执行的命令“，变成”具有执行权限的命令“了。从而可以在系统内任意执行Bash命令语句，胡作非为（相当于获得root超级用户权限）。

1. 正常执行过程
2. 作为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。
3. Bash还有一种使用环境变量来定义函数的方法，这是它的特性。



1. 如果环境变量的值以字符"() {"开头，那么这个变量就会被当作是一个导入函数的定义（Export），这种定义只有在shell启动的时候才生效。
2. 利用存在漏洞版本的bash用export引入触发ShellShock

六．漏洞可能会带来的影响

1. 此漏洞可以绕过ForceCommand在sshd中的配置，从而执行任意命令。

2. 如果CGI脚本用bash编写，则使用mod\_cgi或mod\_cgid的Apache服务器会受到影响。

3. DHCP客户端调用shell脚本来配置系统，可能存在允许任意命令执行。

4. 各种daemon和SUID/privileged的程序都可能执行shell脚本，通过用户设置或影响环境变量值，允许任意命令运行。

六．感想

安全难以完美，更因为时间并不站在防御者这一边。无论是攻击包一击必杀的闪电战，还是威胁的长期潜伏，都是如此。

作为一名学习网络安全方面专业的学生，我们更应该提高警惕，提高自身的能力