**Shellshock 漏洞分析与利用**

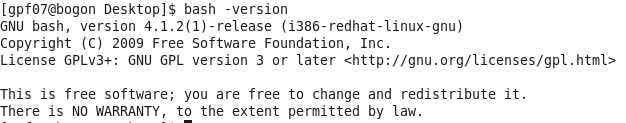
1. **漏洞介绍**

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。它的原理是利用了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。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。这可使攻击者在未授权的情况下访问计算机系 统。此漏洞的影响对象为 Bash 1.14~Bash 4.3 的 Linux/Unix 系统。

**二、漏洞复现**

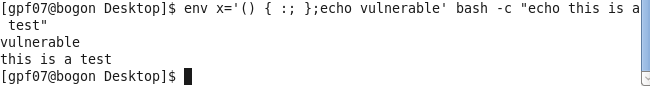
1、检查 Linux 的 bash 版本号

输入$bash –version



此漏洞只对 Linux 系统 bash 版本 1.14~4.3 有影响，所以在复现漏洞前，先对当前 Linux 的 bash 版本号进行检验。有图可见，此 Linux 的 bash 版本为 4.1.2 可以实现。

2. 检测此漏洞是否存在



如果输出vulnerable,说明bash有漏洞。

3. 漏洞复现

Bash 读取了环境变量，在定义 foo 之后就直接调用了后面的函数，一旦调用 bash，自定义语句就直接触发

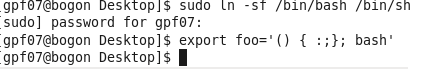
利用 shellshock 漏洞来获取权限

①输入 sudo ln -sf /bin/bash /bin/sh：使/bin/sh 指向/bin/bash

②编写如下 c 代码：



③利用漏洞



④无需密码直接获取 root



**三、漏洞危害**

这次的漏洞是系统级别的，并不是针对于数据或安全证书存在相应的风险漏洞，美国国家标准与技术研究所将 Shellshock 漏洞的严重性、影响力和可利用性评为最高的 10 分，同时对其复杂性的评分较低，这意味着黑客可以相对容易地利用这一漏洞。