CVE-2014-6271——bash破壳漏洞复现

漏洞复现：

检查当前 Linux的 bash 版本

Bash版本小于等于4.3可能存在漏洞

可以使用如下命令查看bash版本：bash -version

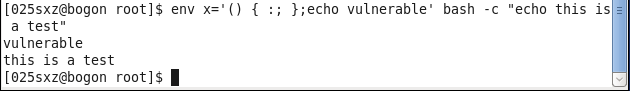


检测此漏洞是否存在

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

若存在漏洞，将会回显：

1. vulnerable
2. This is a test



漏洞原理：

目前的Bash使用的环境变量是通过函数名称来调用的，导致漏洞出问题是以“(){”开头定义的环境变量在命令ENV中解析成函数后，Bash执行并未退出，而是继续解析并执行shell命令。而其核心的原因在于在输入的过滤中没有严格限制边界，也没有做出合法化的参数判断。

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。