# shellshock漏洞分析

## 一．漏洞简介

**Shellshock**，又称**Bashdoor**，是在[Unix](https://baike.baidu.com/item/Unix" \t "https://baike.baidu.com/item/Shellshock/_blank)中广泛使用的Bash shell中的一个[安全漏洞](https://baike.baidu.com/item/%E5%AE%89%E5%85%A8%E6%BC%8F%E6%B4%9E/2890124" \t "https://baike.baidu.com/item/Shellshock/_blank)，首次于2014年9月24日公开。许多互联网[守护进程](https://baike.baidu.com/item/%E5%AE%88%E6%8A%A4%E8%BF%9B%E7%A8%8B" \t "https://baike.baidu.com/item/Shellshock/_blank)，如网页服务器，使用bash来处理某些命令，从而允许攻击者在易受攻击的Bash版本上执行任意代码。这可使攻击者在未授权的情况下访问计算机系统。

## 漏洞原理

Shellshock是一个特权升级漏洞，它为系统用户提供了执行应该不可用的命令的方法。这是通过Bash的“函数导出”功能发生的，因此在一个运行的Bash实例中创建的命令脚本可以与下级实例共享。通过在实例之间共享的表内编码脚本（称为[环境变量](https://baike.baidu.com/item/%E7%8E%AF%E5%A2%83%E5%8F%98%E9%87%8F" \t "https://baike.baidu.com/item/Shellshock/_blank)列表）来实现此功能。Bash的每个新实例都会扫描此表以获取编码脚本，将每个实例组装成一个在新实例中定义该脚本的命令，然后执行该命令。新实例假设在列表中找到的脚本来自另一个实例，但是它不能验证这个，也不能验证它构建的命令是一个正确形成的脚本定义。因此，攻击者可以在系统上执行任意命令，或利用Bash命令解释器中可能存在的其他错误（如果攻击者有办法操纵环境变量列表并导致Bash运行）。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。如果要达到远程代码执行的目的，必须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。

## 漏洞复现

漏洞代码：

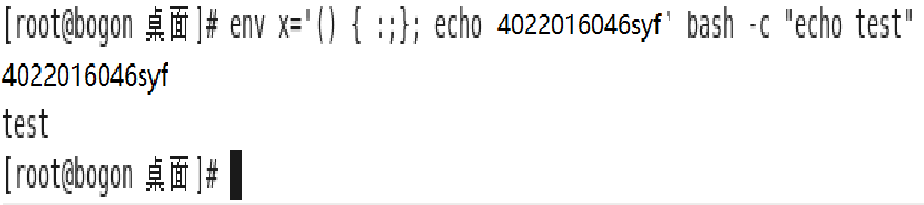
|  |  |
| --- | --- |
| 1 2 3 | /builtins/common.h #define SEVAL\_FUNCDEF 0x080 /\* onlyallow function definitions \*/  #define SEVAL\_ONECMD 0x100 /\* onlyallow a single command |
| 1 2 3 4 5 6 7 8 | \*//builtins/evalstring.c if((flags & SEVAL\_FUNCDEF) && command->type != cm\_function\_def)  {  internal\_warning("%s: ignoring function definition attempt", from\_file);  should\_jump\_to\_top\_level= 0;  last\_result= last\_command\_exit\_value = EX\_BADUSAGE;  break;  } |

1/builtins/evalstring.c

2if (flags & SEVAL\_ONECMD)

3 break;

漏洞实现：



## 漏洞影响

Shellshock错误将影响[Bash](https://baike.baidu.com/item/Bash" \t "https://baike.baidu.com/item/Shellshock/_blank)，即各种基于[Unix](https://baike.baidu.com/item/Unix" \t "https://baike.baidu.com/item/Shellshock/_blank)的系统用来执行命令行和命令脚本。它通常安装为系统的默认[命令行界面](https://baike.baidu.com/item/%E5%91%BD%E4%BB%A4%E8%A1%8C%E7%95%8C%E9%9D%A2" \t "https://baike.baidu.com/item/Shellshock/_blank)。对Bash的[源代码](https://baike.baidu.com/item/%E6%BA%90%E4%BB%A3%E7%A0%81" \t "https://baike.baidu.com/item/Shellshock/_blank)历史的分析显示自1989年9月Bash版本1.03发布以来，这些bug已经存在。