

发现我用的debian版本里的BASH版本并不存在该漏洞

漏洞的关键在于bash会把定义的各种函数放到env里面去，大致的格式如下：

function foo { echo bar; }

export -f foo

env | grep -A1 foo

foo=() { echo bar

}

这里的关键在于，这里它执行函数的时候，不是检测完整的“{}”对，而是简单的执行“{”之后的所有bash代码，也包括放进去的代码。

但我在添加的打印pengyang并没有被执行，所以我觉得可能是我下载的debian版本中该漏洞已经被修复。