Linux程序设计期中报告
Linux著名漏洞 – Shellshock

谢志彬, 6103115112, 计科153
2018/05/01

Abstract—Shellshock，又称Bashdoor，是在Unix中广泛使用的Bash shell中的一个安全漏洞

Index Terms—Linux, Bash, Bug, 漏洞

1 简介

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。

许多互联网守护进程，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

– 维基百科

2 漏洞信息

漏洞英文名称: Bash Shellshock
中文命名: 破壳（X-CERT）
威胁响应等级: A级
漏洞相关CVE编号: CVE-2014-6271
漏洞发现者: Stéphane Chazelas（法国）
漏洞发现事件: 2014年9月中旬
漏洞公布时间: 9月25日
漏洞影响对象: bash 1.14至bash 4.3的Linux/Unix系统

3 背景

Shellshock错误将影响Bash，即各种基于Unix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。对Bash的源代码历史的分析显示自1989年9月Bash版本1.03发布以来，这些bug已经存在。

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）。

2014年9月24日向公众发布了这个bug，当时Bash更新了这个修补程序，准备发布尽管需要一些时间来更新计算机来解决潜在的安全问题。

4 漏洞起源

漏洞信息最早来源于国外知名漏洞网站exploit-db下的第34765篇漏洞报告，其中出现了一条验证命令：

env x='() :;; echo vulnerable' bash -c "echo this is a test"

如果在一个含有版本号小于bash 4.3的linux或者unix系统上执行以上命令，可能会得到以下输出：

vulnerable
this is a test

其中如果出现第一行vulnerable则说明该系统存在一个由bash程序缺陷导致的任意命令执行漏洞。

5 漏洞原理及分析

该脚本的出现引起了技术人员的极大关注，其中env为一个系统命令，该命令让系统创建一个环境变量

x='() :;; echo vulnerable'

- *Symantec Security Response*
  E-mail: see https://www.symantec.com/
- *Unix & Linux on stackexchange.*
- *CSDN的pygain*

并且带着这个环境变量的值执行

bash -c "echo this is a test"

第一行输出的*"vulnerable"*暴露了漏洞的存在

因为函数定义*'() :;;'*之后的*'echo vulnerable'*指令本不该被执行却被执行。

对bash详细分析后得知bash在处理含有函数定义诸如*"() :;;"*的环境变量赋值的代码上存在设计缺陷，错误地将函数定义后面的字符串作为命令执行。

所以真正的利用与env命令无关，只要设法让系统接受一个含有*"[函数定义]+[任意命令]"*的环境变量赋值则可触发"[任意命令]"部分所表示的代码执行。

6 影响范围

对于存在Bash漏洞系统而言，由于它允许未经授权的远程用户可以指定Bash环境变量，那么运行这些服务或应用程序的系统，就存在漏洞被利用的可能。

只要是能通过某种手段为bash传递环境变量的程序都受此影响。当然最典型的的就是bash写的CGI程序了，客户端通过在请求字符串里加入构造的值，就可以轻松攻击运行CGI的服务器。

目前大多数的网站很少用CGI了，所以问题不算太大。但是有很多的网络设备，如路由器、交换机等都使用了Perl或者其他语言编写的CGI程序，只要是底层调用了bash，那么就爱存在风险。

任何已知程序，只要满足以下两个条件就可以被用来通过bash漏洞导致任意命令执行：

- 程序在某一时刻使用bash作为脚本解释器处理环境变量赋值
- 环境变量赋值字符串的提交取决于用户输入

目前，可能被利用的系统包括：

- 运行CGI脚本（通过mod_cgi 和 mod_cgid）的Apache HTTP 服务器
- 使用CGI作为网络接口的基于Linux的路由器
- 使用Bash的各种嵌入式设备
- 某些DHCP客户端
- 使用Bash的各种网络服务
- 使用 ForceCommand 功能的 OpenSSH 服务器

7 该漏洞如何被利用

虽然此漏洞可能会影响任何运行Bash的计算机，但它只能在特定情况下被远程攻击者利用。要成功发生攻击，攻击者需要强制应用程序向Bash发送恶意环境变量。

最可能的攻击途径是通过使用CGI（通用网关接口）的Web服务器，这是广泛使用的用于生成动态Web内容的系统。攻击者可能使用CGI将恶意的环境变量发送给易受攻击的Web服务器。因为服务器使用Bash来解释变量，所以它也会运行任何恶意的命令。

攻击者在Web服务器上成功利用此漏洞的后果是严重的。例如，攻击者可能有能力转储密码文件或将恶意软件下载到受感染的计算机上。一旦进入受害者的防火墙，攻击者就可以危害并感染网络上的其他计算机。

除了Web服务器之外，其他易受攻击的设备还包括使用CGI Web界面的基于Linux的路由器。与对Web服务器的攻击一样，CGI可能会被利用来利用此漏洞并向路由器发送恶意命令。

运行Mac OS X的计算机也可能存在漏洞，直到Apple发布针对此漏洞的修补程序。同样，攻击者需要找到一种方法将错误的命令传递给目标Mac上的Bash。攻击OS X的最可能途径可能是通过安全通信协议Secure Shell（SSH）。但是，似乎攻击者需要有效的SSH凭据才能执行攻击。换句话说，他们必须已经登录到SSH会话。

物联网（IoT）和嵌入式设备（如路由器）在运行Bash时可能会受到攻击。然而，许多新设备运行一组称为BusyBox的工具，它提供了Bash的替代方案。运行BusyBox的设备不容易受到Bash Bug攻击。

8 如何修复该漏洞

修复此漏洞的最简单方法是使用默认包管理器更新Bash的版本。

Debian

sudo apt update

sudo apt install –only-upgrade bash

Fedora, Red Hat, Cent OS等.

yum -y update bash

9 结束语

以上是所有关于Shellshock的内容。
论文基于IEEE Latex 模板编写

REFERENCES

[1] *Shellshock (software bug) - Wikipedia*
[2] *ShellShock: All you need to know about the Bash Bug vulnerability*
[3] *Trend Micro products and the Shellshock – Linux Bash Vulnerability (Bash Bug) (CVE-2014-6271) and (CVE-2014-7169)*