密级	公开

破壳漏洞（ShellShock）应急概要

[第三版 2014/9/27 下午]

知道创宇安全研究团队

1. 更新情况

版本	时间	描述
第一版	2014/9/26 中午	第一版完成。
第二版	2014/9/26 下午	1. 新增加速乐防御平台的攻击统计细节； 2. 完善修复建议；
第三版	2014/9/27 下午	1. 破壳漏洞官网出现：shellshocker.net 2. 更新：漏洞概要； 3. 新增补丁绕过后（CVE-2014-7169）的漏洞源码级分析； 4. 新增ZoomEye第四组数据：某NAS漏洞情况； 5. 新增ZoomEye第五组数据：某安全网关漏洞情况； 6. 完善修复建议； 7. 新增：相关资源链接；

2. 漏洞概要

2014 年 9 月 24 日，Bash 惊爆严重安全漏洞，编号为 **CVE-2014-6271**，该漏洞将导致远程攻击者在受影响的系统上执行任意代码。

GNU Bash 是一个为 GNU 计划编写的 Unix Shell，广泛使用在 Linux 系统内，最初的功能仅是一个简单的基于终端的命令解释器。

漏洞描述：GNU Bash 4.3 及之前版本在评估某些构造的环境变量时存在安全漏洞，向环境变量值内的函数定义后添加多余的字符串会触发此漏洞，攻击者可利用此漏洞改变或绕过环境限制，以执行 Shell 命令。某些服务和应用允许未经身份验证的远程攻击者提供环境变量以利用此漏洞。此漏洞源于在调用 Bash Shell 之前可以用构造的值创建环境变量。这些变量可以包含代码，在 Shell 被调用后会被立即执行。

这个漏洞的中文名被 XCERT 命名为：破壳漏洞，英文是：ShellShock。

破壳漏洞的严重性被定义为 10 级（最高），今年 4 月爆发的 OpenSSL“心脏出血”漏洞才 5 级！

破壳漏洞存在有 20 年。

漏洞影响：GNU Bash <= 4.3，此漏洞可能会影响到：

注：以下几点参考自：

https://raw.githubusercontent.com/citypw/DNFWAH/master/4/d4_0x07_DNFWAH_shellshock_bash_story_cve-2014-6271.txt，且结论经过我们验证有效。

- 在 SSHD 配置中使用了 ForceCommand 用以限制远程用户执行命令，这个漏洞可以绕过限制去执行任何命令。一些 Git 和 Subversion 部署环境的限制 Shell 也会出现类似情况，OpenSSH 通常用法没有问题。
- Apache 服务器使用 mod_cgi 或者 mod_cgid，如果 CGI 脚本在 BASH 或者运行在子 Shell 里都会受影响。子 Shell 中使用 C 的 system/popen，Python 中使用 os.system/os.popen，PHP 中使用 system/exec(CGI 模式)和 Perl 中

使用 open/system 的情况都会受此漏洞影响。

- PHP 脚本执行在 mod_php 不会受影响。
- DHCP 客户端调用 Shell 脚本接收远程恶意服务器的环境变量参数值的情况会被此漏洞利用。
- 守护进程和 SUID 程序在环境变量设置的环境下执行 Shell 脚本也可能受到影响。
- 任何其他程序执行 Shell 脚本时用 Bash 作为解释器都可能受影响。Shell 脚本不导出的情况下不会受影响。

漏洞验证，可以使用如下命令来检查系统是否存在此漏洞（在本机 Bash 环境下运行）：

CVE-2014-6271 测试方式：

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

如执行结果如下表明有漏洞：

```
vulnerable
this is a test
```

注：CVE-2014-6271 的漏洞源码级分析请参考：

http://blog.knownsec.com/2014/09/bash_3-0-4-3-command-exec-analysis/

修补后，又被绕过，CVE-2014-7169 最新测试方法：

```
env -i    X='() { (a)=>\' bash -c 'echo date'; cat echo
```

如执行结果如下则仍然存在漏洞：

```
bash: X: line 1: syntax error near unexpected token `='
bash: X: line 1: `'
bash: error importing function definition for `X'
Wed Sep 24 14:12:49 PDT 2014
```

注：CVE-2014-7169 的漏洞源码级分析请参考：

http://blog.knownsec.com/2014/09/bash_3-0-4-3-command-exec-patch-bypas

s-analysis/

可能还会有新的绕过方式，时刻保持关注！

3. ZoomEye 应急概要

这个破壳漏洞确实是一个危害极大的漏洞，胜于今年 4 月 8 号爆发的“心脏出血”，但破壳漏洞的探测方式很复杂，不同的组件测试方式有所区别，很难评估一个影响面，但是可以肯定的是 Bash<=4.3 版本都受影响，而 Bash 在至少百亿级别数量的设备上使用，因为 Bash 是最流行的 Linux Shell。

来自知道创宇的 ZoomEye 团队（钟馗之眼网络空间探知系统）通过几种方式的组合检测，得到了些影响结论。

注意：以下这些影响都是可被直接远程攻击的，属于高危级别！

3.1. 第一组数据

我们发现**某厂商的应用交付管理系统**存在破壳漏洞，经过 ZoomEye 的特殊探测，大陆地区范围内有 **13254** 台设备受到破壳漏洞影响，可被直接远程攻击。

利用破壳漏洞，可以直接拿到服务器 root 权限。

3.2. 第二组数据

经过 ZoomEye 的 Fuzzing 探测，Fuzzing 列表如下：

```
/cgi-bin/load.cgi
/cgi-bin/gsweb.cgi
/cgi-bin/redirector.cgi
/cgi-bin/test.cgi
/cgi-bin/index.cgi
/cgi-bin/help.cgi
/cgi-bin/about.cgi
/cgi-bin/vidredirect.cgi
/cgi-bin/click.cgi
/cgi-bin/details.cgi
/cgi-bin/log.cgi
/cgi-bin/viewcontent.cgi
/cgi-bin/content.cgi
```

/cgi-bin/admin.cgi
/cgi-bin/webmail.cgi

全球大概存在 **142000** 主机受影响，需要注意的是由于 Fuzzing 规则不完备，得到的数量肯定会不完备，但这个数字至少可以看到可被直接远程攻击利用的面很大。

3.3. 第三组数据

我们看到 masscan 的官方发布了消息：

http://blog.erratasec.com/2014/09/bash-shellshock-bug-is-wormable.html

他们全球探测的结论是：至少 **150 万**受影响，而这验证规则很简单，仅对主机的 80 端口进行直接请求，这个结论我们也在验证。

3.4. 第四组数据

我们发现某公司的 NAS 存储设备存在破壳漏洞，ZoomEye 针对某 NAS 的 8080 端口进行大规模探测，目前的进度如下：

国家/地区	受影响数量（台主机）
日本	5158
台湾	4579
香港	2492

利用破壳漏洞，可以拿下某 NAS 的 admin 权限（最高）。

3.5. 第五组数据

我们发现某厂商的安全网关等产品存在破壳漏洞，ZoomEye 针对相关设备的 80 端口进行大规模探测，在大陆地区发现 **71** 台受影响设备。

利用破壳漏洞，可以拿下相关设备 root 权限。

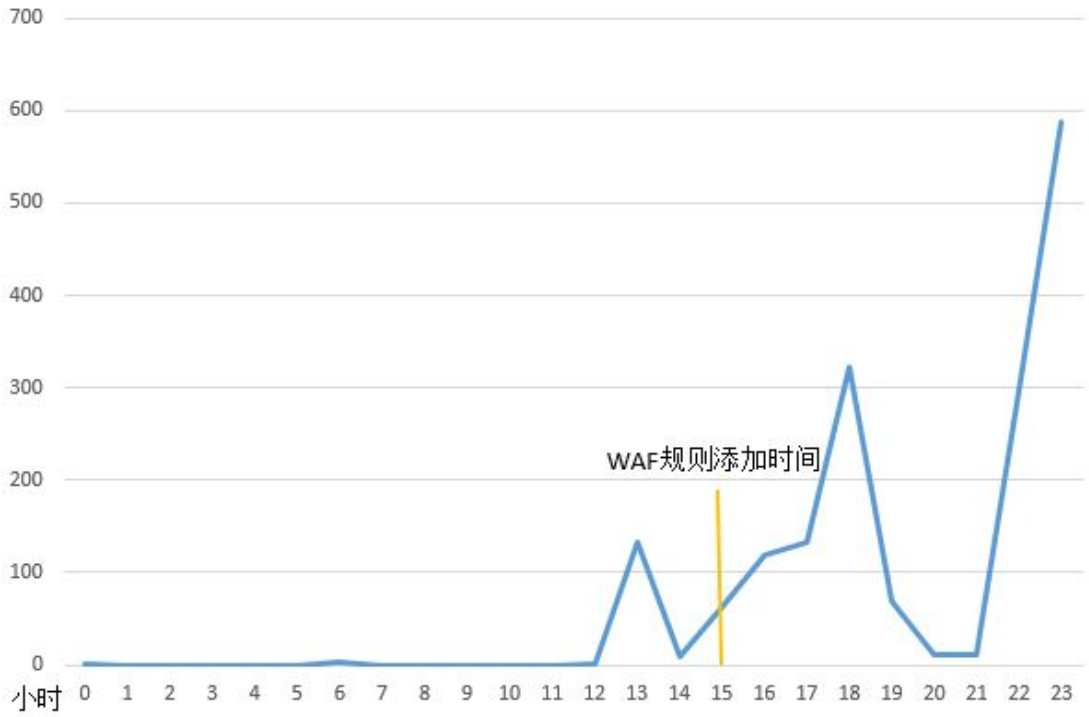
可以从这几组数据看到，探测方式各不相同，如果继续扩展可以逐步描绘出越来越清晰的影响面（**可直接远程攻击**），更多成果还在继续。

4. 加速乐云防御平台应急概要

截止时间 2014/9/26 12:00 的统计如下：

来自知道创宇加速乐团队的应急情况，拦截了 **1759** 次破壳漏洞攻击！

下图为昨日破壳漏洞按小时活跃趋势图：



从图中可见，加速乐云防御平台在漏洞爆发之前就已经添加规则。

昨日拦截情况如下：

总共拦截数：1,759 次

受攻击站点数：214 个

攻击成功站点数：0 个

发起攻击 IP 数：6 个

从加速乐云防御平台可以侧面看出，这种漏洞的疯狂情况。

5. 其他结论

通过我们连夜分析，还有一些可靠结论可以作为参考：

1. 破壳漏洞的蠕虫已经开始全球蔓延，应该是利用 masscan 来进行大规模植入的。

蠕虫代码在这：

https://gist.github.com/anonymous/929d622f3b36b00c0be1

2. DHCP 服务受影响，这个意味着这个破壳漏洞绝不仅 Linux 服务器的事！

POC 细节在这：

https://www.trustedsec.com/september-2014/shellshock-dhcp-rce-proof-concept/

3. 好几家著名厂家已经发布修复公告。

例如：

Akamai（全球最大的 CDN 服务商）：

https://blogs.akamai.com/2014/09/environment-bashing.html

GitLab：

https://about.gitlab.com/2014/09/24/gitlab-shell-and-bash-cve-2014-6271/

4. 基于 SIP 协议的破壳漏洞扫描也开始了！

https://github.com/zaf/sipshock

6. 修复建议

现在可以按照下面方式进行 Bash 的升级修复：

操作系统	升级方式
Ubuntu/Debian	apt-get update apt-get install bash
RedHat/CentOS/Fedora	yum update -y bash
Arch Linux	pacman -Syu

OS X	brew update brew install bash sudo sh -c 'echo "/usr/local/bin/bash" >> /etc/shells' chsh -s /usr/local/bin/bash sudo mv /bin/bash /bin/bash-backup sudo ln -s /usr/local/bin/bash /bin/bash
MacPorts	sudo port self update sudo port upgrade bash

建议升级后按上面的方法诊断是否补丁完全。

7. 相关资源链接

1. ShellShock 官网：https://shellshocker.net/
2. 知道创宇官网：http://www.knownsec.com/
3. 知道创宇旗下 - ZoomEye 官网：http://www.zoomeye.org/
4. 知道创宇旗下 - 加速乐云防御平台官网：http://www.jiasule.com/