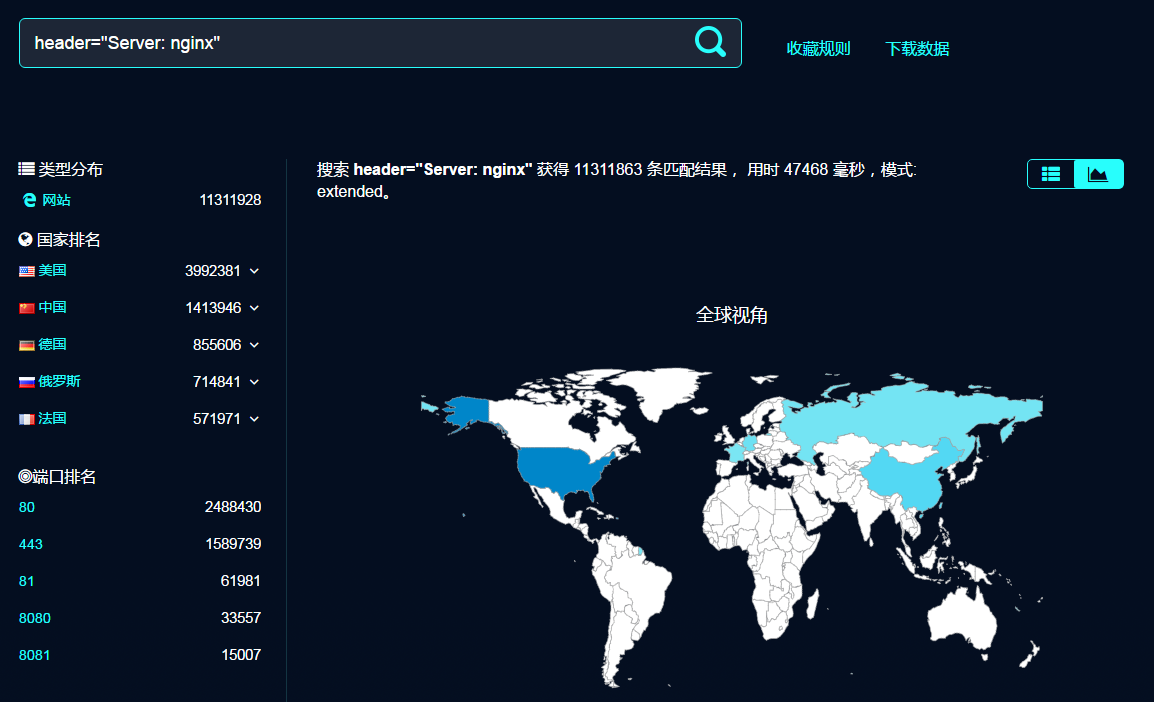
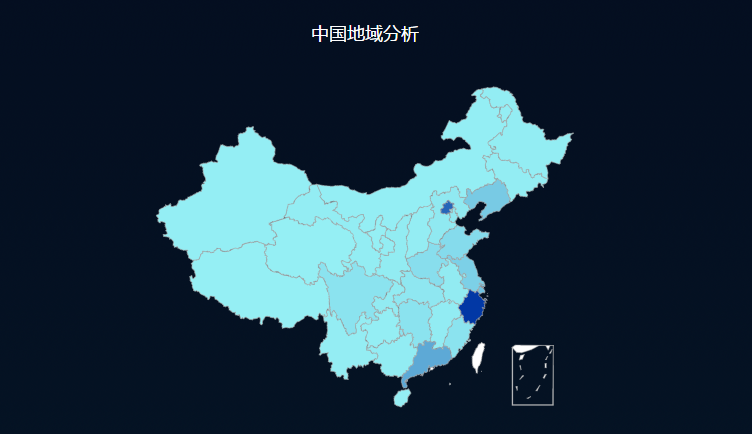
**Debian（ubuntu）发行版Nginx本地提权漏洞**

2016年10月25日Debian网站发布Nginx权限提升漏洞，在1.6.2-5+deb8u3版本中修复此漏洞。2016年11月15日，Poc在网络发布。影响范围广，提醒nginx低版本尽快升级。

Nginx ("engine x") 是一个高性能的HTTP和反向代理服务器，也是一个IMAP/POP3/SMTP服务器。全球使用广泛，各大厂商均有使用。根据白帽汇fofa.so的最新数据显示，目前互联网中公网使用的nginx有11311863个。其中中国地区top5为浙江 99785，北京 302019，广东 153632，上海 97380，辽宁 79897。



Nginx全球分布



Nginx中国分布

**原理与危害**

Nginx服务器在Debian-based为基础的Debian和ubuntu系统上可以以高权限创建日志目录，攻击者可以利用nginx从本地用户权限提升至root权限。恶意攻击者可以提升至最高的root权限。完全控制服务器。

**漏洞影响**

Debian(Ubuntu)的nginx低版本中存在该问题

**CVE编号**

CVE-2016-1247

**漏洞分析**

基于Debian系统默认安装的nginx会创建/var/log/nginx/目录，该目录的所有者是www-data，本地攻击者可以通过符号链接到任意文件来替换日志文件，从而实现提权。当通过替换符号链接的日志文件后，需要等待nginx daemon重新打开日志文件。故这里需要对nginx进行重启或者daemon 接收到USR1的处理信号。

USR1会通过基于debian的系统中默认安装的logrotate脚本调用do\_rotate（）函数自动发送。

相关内容如下：

--------[ /etc/logrotate.d/nginx ]--------

/var/log/nginx/\*.log {

daily

missingok

rotate 52

compress

delaycompress

notifempty

create 0640 www-data adm

sharedscripts

prerotate

if [ -d /etc/logrotate.d/httpd-prerotate ]; then \

run-parts /etc/logrotate.d/httpd-prerotate; \

fi \

endscript

postrotate

invoke-rc.d nginx rotate >/dev/null 2>&1

endscript

}

------------------------------------------

----------[ /etc/init.d/nginx ]-----------

[...]

do\_rotate() {

start-stop-daemon --stop --signal USR1 --quiet --pidfile $PID --name $NAME

return 0

}

[...]

通过上面内容我们可以看到logrotation脚本会在corn中每天6:25AM自动调用，因此如果/etc/logrotate.d/nginx已经设置了'daily'日志回滚，攻击者将在不需要重启，在24小时内实现提权到ROOT。

**漏洞利用代码（PoC）**

利用方式：

*./nginxed-root.sh path\_to\_nginx\_error.log*

代码见同目录下的nginxed-root.sh文件。

执行效果如下图：



**修复建议**

1. 使用已经有修复补丁的版本

已经修复的版本如下：

Debian:

在Nginx 1.6.2-5+deb8u3中修复

Ubuntu:

Ubuntu 16.04 LTS:

在1.10.0-0ubuntu0.16.04.3中修复

Ubuntu 14.04 LTS:

在1.4.6-1ubuntu3.6中修复

Ubuntu 16.10:

在1.10.1-0ubuntu1.1中修复

更新地址<https://www.debian.org/security/2016/dsa-3701>

<https://www.ubuntu.com/usn/usn-3114-1/>

白帽汇会持续对该漏洞进行跟进。

**参考**

[1] <http://legalhackers.com/advisories/Nginx-Exploit-Deb-Root-PrivEsc-CVE-2016-1247.html>

[2] <https://www.debian.org/security/2016/dsa-3701>

[3] <https://www.ubuntu.com/usn/usn-3114-1/>

[4] <https://legalhackers.com/exploits/CVE-2016-1247/nginxed-root.sh>