Nginx近期漏洞报告

**0001**

.漏洞名称：Nginx 权限提升漏洞 (Debian、Ubuntu发行版)

漏洞时间：2016-11-16

CVE-ID：CVE-2016-1247

影响平台：Debian、Ubuntu发行版

影响版本：

Debian: Nginx1.6.2-5+deb8u3  
Ubuntu 16.04: Nginx1.10.0-0ubuntu0.16.04.3  
Ubuntu 14.04: Nginx1.4.6-1ubuntu3.6  
Ubuntu 16.10: Nginx1.10.1-0ubuntu1.1

介绍：发现基于Debian或Debian等基于Debian的发行版上的Nginx Web服务器打包创建的日志目录具有不安全的权限，恶意本地攻击者可以利用该目录来将其特权从nginx / web用户（www-data）升级为root

攻击web应用程序之后获得到www-data的账户访问权限之后可以很容易的利用这个漏洞提升权限至root。

描述;

从基于Debian的系统（Debian，Ubuntu等）上的默认存储库安装的Nginx在以下位置并具有以下权限创建nginx日志目录：

root@xenial:~*# ls -ld /var/log/nginx/*

drwxr-**x**--- 2 www-data adm 4096 Nov 12 22:32 /var/**log**/nginx/

root@xenial:~*# ls -ld /var/log/nginx/\**

-rw-r----- 1 www-data adm 0 Nov 12 22:31 /var/**log**/nginx/access.**log**

-rw-r--r-- 1 root root 0 Nov 12 22:47 /var/**log**/nginx/error.**log**

由于/ var / log / nginx目录归www-data所有，因此本地攻击者可以通过Nginx（或服务器本身）上运行的Web应用程序中的漏洞获取对系统的访问权限，以替换日志文件与指向任意文件的符号链接。

在nginx启动/重启后，日志将被写入符号链接指向的文件中。

这使攻击者可以将特权升级为root用户。

设法用符号链接替换日志文件的攻击者必须等待nginx守护程序重新打开日志文件。为此，需要重新启动nginx服务，或者守护程序需要接收USR1进程信号。

但是，USR1是在默认安装的基于Debian的系统上通过logrotate脚本自动发送的，该脚本调用do\_rotate（）函数。

在默认的Ubuntu / Debian安装中，每天早上6：25，cron.daily每天都会调用一次logrotation脚本。

如果将/etc/logrotate.d/nginx设置为“每天”轮换日志，则攻击者可以在下次轮换日志后24小时内获得root特权，而无需任何系统管理员交互。

POC：CVE-2016-1247（非pocsuite插件）

**0002**

漏洞名称：Nginx远程整数溢出漏洞

漏洞时间：2017-07-13

CVE-ID：CVE-2017-7529

影响平台：linux、Windows

影响版本： 0.5.6 <=version<=1.13.2

介绍：在Nginx范围过滤器中发现了一个安全问题。特制的请求可能会导致整数溢出和范围的不正确处理，从而可能导致敏感信息泄漏（CVE-2017-7529）。

当将nginx与标准模块一起使用时，如果从缓存返回了响应，则攻击者可以获取缓存文件头。在某些配置中，缓存文件头可能包含后端服务器的IP地址或其他敏感信息。

此外，使用第三方模块，该问题有可能导致拒绝服务或泄露工作进程内存。目前尚无此类模块。

该问题影响nginx 0.5.6-1.13.2。此问题已在nginx 1.13.3、1.12.1中修复。

EXP or POC：CVE-2017-7529（python）