链滴

Nginx 修复漏洞打补丁过程

作者：imaojun

原文链接：https://ld246.com/article/1557727858253

来源网站：链滴

漏洞报告

最近收到安全部门的安全扫描报告。内容如下：

nginx 安全漏洞（CVE-2018-16845） 中危 nginx类nginx是由俄罗斯的程序设计师Igor Sysoev开发的一款轻量级Web服务器/反向代理服务器及电子邮件（IMAP/POP3）代理服务器。 Nginx 1.155及之前的版本和1.14.1版本中的ngx_http_mp4_module组件存在内存泄露漏洞，该漏洞源于程序没正确处理MP4文件。远程攻击者可利用该漏洞获取敏感信息或造成拒绝服务。 厂商补丁: 目前厂商发布升级补丁以修复漏洞，补丁获取链接： http://mailman.nginx.org/pipermail/nginx-announce2018/000221.html

一个高危漏洞，赶紧网上查询下资料这准备修复。

修复过程

去补丁地址获取补丁,可以看到这个内容：

Patch for the issue can be found here:

http://nginx.org/download/patch.2018.mp4.txt

点击获取查看补丁信息：

```
--- src/http/modules/ngx_http_mp4_module.c
+++ src/http/modules/ngx_http_mp4_module.c
@@ -942,6 +942,13 @@ ngx_http_mp4_read_atom(ngx_http_mp4_file
             atom_size = ngx_mp4_get_64value(atom_header + 8);
             atom_header_size = sizeof(ngx_mp4_atom_header64_t);

+            if (atom_size < sizeof(ngx_mp4_atom_header64_t)) {
+                ngx_log_error(NGX_LOG_ERR, mp4->file.log, 0,
+                              "\"%s\" mp4 atom is too small:%uL",
+                              mp4->file.name.data, atom_size);
+                return NGX_ERROR;
+            }
+
         } else {
             ngx_log_error(NGX_LOG_ERR, mp4->file.log, 0,
                           "\"%s\" mp4 atom is too small:%uL",
```

第一行和第二行表示漏洞发生的文需要修改的文件

第三行表示修复前的漏洞位置在942行的后6行，942，13为补丁添加的位置到第13行

真正需要添加的部分为+号部分，复制定漏洞文件需要删除+号（+表示新增）

接着去nginx的启动文件夹，查看编译参数信息：

./nginx -V

得到如下信息:

nginx version: nginx/1.11.5 built by gcc 4.8.5 20150623 (Red Hat 4.8.5-36) (GCC) built with OenSSL 1.0.1c 10 May 2012 TLS SNI support enabled configure arguments: --prefix=/app/nginx

```
nginx --with-pcre=/app/nginx/soft/pcre-8.35 --with-zlib=/app/nginx/soft/zlib-1.2.8 --with-openssl=/app/nginx/soft/openssl-1.0.1c --with-http_ssl_module --with-http_realip_module
```

需要用到的内容为configure arguments:后的内容

去nginx源码目录编译

```
cd nginx-1.11.5 && ./configure --prefix=/app/nginx/nginx --with-pcre=/app/nginx/soft/pcre8.35 --with-zlib=/app/nginx/soft/zlib-1.2.8 --with-openssl=/app/nginx/soft/openssl-1.0.1c --ith-http_ssl_module --with-http_realip_module  && make
```

注意：不要make install,不然会覆盖现有的

等待编译成功后会生成一个objs目录，进入目录

```
cd objs
```

复制编译生成的可执行文件到原先的nginx的sbin目录

```
cp nginx /app/nginx/nginx/sbin
```

注意，复制前建议先备份原有的sbin文件

切换进程:

```
make upgrade
```

或者去替换的sbin目录

```
,./nginx -s reload
```

原文链接：Nginx 修复漏洞打补丁过程