链滴

记录 CVE-2020-1971: OpenSSL 拒绝服务漏洞解决过程

作者：Jireh

原文链接：https://ld246.com/article/1607587864910

来源网站：链滴

腾讯云发来了通知发现有新的高危漏洞CVE-2020-1971

漏洞描述：

2020年12月08日，OpenSSL官方发布安全公告，披露CVE-2020-1971 OpenSSL GENERAL_NAME_mp 拒绝服务漏洞。当两个GENERAL_NAME都包含同一个EDIPARTYNAME时，由于GENERAL_NAE_cmp函数未能正确处理，从而导致空指针引用，并可能导致拒绝服务。

腾讯安全专家建议受影响的OpenSSL用户尽快采取安全措施阻止漏洞攻击。

OpenSSL是一个开放源代码的软件库包，应用程序可以使用这个包来进行安全通信，避免窃听，同时认另一端连接者的身份。这个包广泛被应用在互联网的网页服务器上。

受影响的版本：

OpenSSL 1.1.1 ~ 1.1.1h

OpenSSL 1.0.2 ~ 1.0.2w

安全版本：

OpenSSL 1.1.1i

OpenSSL 1.0.2x

原文链接：记录 CVE-2020-1971: OpenSSL 拒绝服务漏洞解决过程

解决过程

官方给的解决办法就是升级版本，只要把服务器上OpenSSL版本升级到安全的版本就行了。

```
[root@VM_0_7_centos /]# openssl version
OpenSSL 1.0.2k-fips  26 Jan 2017
```

登上服务器确认了下，openssl版本的确是在受影响的范围内，那接下是要升级版本就可以了

升级安装

```
cd /usr/local/src/

wget https://www.openssl.org/source/openssl-1.1.1i.tar.gz

yum install -y zlib

tar zxf openssl-1.1.1i.tar.gz

cd openssl-1.1.1i/

./config --prefix=/usr/local/openssl shared zlib

make depend

make && make install

mv /usr/bin/openssl /usr/bin/openssl.bak

mv /usr/include/openssl /usr/include/openssl.bak

ln -s /usr/local/openssl/bin/openssl /usr/bin/openssl

ln -s /usr/local/openssl/include/openssl /usr/include/openssl

echo /usr/local/openssl/lib >> /etc/ld.so.conf

ldconfig -v
```

最后在输入openssl version检测一下是否升级成功，如果版本号跟选择升级的版本一致，即为升级功

```
[root@VM_0_7_centos bin]# openssl version
OpenSSL 1.1.1i  8 Dec 2020
```