



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](#)

许可协议: [署名-相同方式共享 4.0 国际 \(CC BY-SA 4.0\)](#)

OpenSSL 拒绝服务漏洞(CVE-2020-1971)

漏洞详情

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_cmp 拒绝服务漏洞, 当两个GENERAL_NAME都包含同一个EDIPARTYNAME时, 由于GENERAL_NAME_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。

漏洞类型: 系统组件漏洞

威胁等级: **高危**

修复方案: 将 OpenSSL 升级至最新版本。
检测到服务器存在漏洞风险, 建议立即对相关主机进行快照备份, 避免遭受损失。
[了解快照备份](#)

参考链接: <https://s.tencent.com/research/bsafe/1193.html>

披露时间: 2020-12-09 00:00:00
CVE编号: CVE-2020-1971
CVSS评分: 7.5

影响的服务器

[重新检测](#) [忽略](#) [全部](#) [请选择标签](#)

请输入服务器名称进行搜索

服务器IP/名称	说明	威胁等级	服务器标签	最后检测时间	状态	操作
<input type="checkbox"/> 未命名	OpenSSL版本为 1.0...	高危	暂无标签	2020-12-10 03:47:57	待处理	重新检测 忽略

共 1 条

10 条 / 页

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_cmp 拒绝服务漏洞。当两个GENERAL_NAME都包含同一个EDIPARTYNAME时, 由于GENERAL_NAME_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

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，那接下来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 xzf 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，即为升级成功

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