CentOS平台升级OpenSSL到1.0.1t

我博客服务器使用的OpenSSL是1.0.1e版本，之所以需要升级到OpenSSL 1.0.1t版本是因为1.0.1t版本以下存在一个严重的Bug：Padding oracle in AES-NI CBC MAC check (CVE-2016-2107)，我们可以到这里查看我们的网站是否有这个问题。官方对这个漏洞的描述是：

Padding oracle in AES-NI CBC MAC check (CVE-2016-2107)
==========

Severity: High

A MITM attacker can use a padding oracle attack to decrypt traffic when the connection uses an AES CBC cipher and the server support AES-NI.

This issue was introduced as part of the fix for Lucky 13 padding attack (CVE-2013-0169). The padding check was rewritten to be in constant time by making sure that always the same bytes are read and compared against either the MAC or padding bytes. But it no longer checked that there was enough data to have both the MAC and padding bytes.

OpenSSL 1.0.2 users should upgrade to 1.0.2h
OpenSSL 1.0.1 users should upgrade to 1.0.1t

This issue was reported to OpenSSL on 13th of April 2016 by Juraj Somorovsky using TLS-Attacker. The fix was developed by Kurt Roeckx of the OpenSSL development team.

因为这个Bug我博客HTTPS的SSL安全评分变成了F，所有升级到最新版很有必要了。因为我目前的OpenSSL 1.0.1e所以我直接升级到OpenSSL 1.0.1t即可。下面是安装步骤：

1、下载openssl-1.0.1t

iteblog$ https://www.openssl.org/source/openssl-1.0.1t.tar.gz

2、解压

```
iteblog$ tar -xzvf ./openssl-1.0.1t.tar.gz
iteblog$ cd openssl-1.0.1t/
```

3、配置

```
iteblog$ ./config  --prefix=/usr/local/ssl  --openssldir=/usr/local/ssl
```

4、编译和安装

```
iteblog$ make &&  make install
#建议安装两次，shared 作用是生成动态连接库。
iteblog$ ./config shared --prefix=/usr/local --openssldir=/usr/local/ssl
iteblog$ make clean
iteblog$ make && make install
```

5、检验是否安装成功

```
iteblog$ make &&  make install
#建议安装两次，shared 作用是生成动态连接库。
iteblog$ openssl version
OpenSSL 1.0.1t  3 May 2016
```

如果你看到输出上面的版本，那么你的OpenSSL成功升级了！最后我们重启nginx和php：

```
iteblog$ service nginx stop
Stopping nginx:                            [  OK  ]
iteblog$ service php-fpm stop
Stopping php-fpm:                            [  OK  ]
iteblog$ service php-fpm start
Starting php-fpm:                            [  OK  ]
iteblog$ service nginx start
Starting nginx:                           [  OK  ]
```

我们再去检查一下(CVE-2016-2107)漏洞，现在已经没了。

如果在使用 openssl version 命令出现了以下的异常：

```
iteblog$ openssl version
openssl: error while loading shared libraries: libssl.so.1.1: cannot open shared object file: No s
uch file or directory
```

这是由于 openssl 库的位置不正确造成的。我们可以依次执行以下的命令：

```
iteblog$ ln -s /usr/local/lib64/libssl.so.1.1 /usr/lib64/libssl.so.1.1
iteblog$ ln -s /usr/local/lib64/libcrypto.so.1.1 /usr/lib64/libcrypto.so.1.1
```

然后就可以正常运行了。