CVE-2014-0160分析

diffway / 2017-12-12 19:47:34 / 浏览数 2782 安全技术 漏洞分析 顶(0) 踩(0)

CVE-2014-0160也被成为心脏滴血漏洞，在OpenSSL1.0.1版本中存在严重漏洞，该漏洞会导致内存越界，攻击者可以远程读取存OpenSSL服务器内存中64K的数据
影响版本：OpenSSL1.0.1、1.0.1a、1.0.1b、1.0.1c、1.0.1d、1.0.1e、1.0.1f、Beta 1 of OpenSSL 1.0.2等版本

1 漏洞分析
我这个分析的是openssl-1.0.1.f,下载地址为https://www.openssl.org/source/old/
这里面有所有的老版本我们首先将这个编译，我们现在进行源码查看，我们能从https://bugzilla.redhat.com/attachment.cgi?id=883475&action=diff
查看到官方的修补方案

可以看到主要修改了 d1_both.c 和t1_lib.c 这两个文件中的 dtls1_process_heartbeat(SSL s)
tls1_process_heartbeat(SSL s) 这两个函数从名字可以看出来是处理心跳的，我们从源码中找出这两个函数
我们可以看出 主要是 通过是增加了对 s->s3->rrec.length长度的判断，我们主要看下这个s,s是传入的结构体SSL，我们找到这个这个结构体SSL

我们找到s->s3->rrec.length 中的s3 并看到了是结构体ssl_state_st,并在ssl3_state_st中rrec

这里SSL3_RECORD中记录data和length ,可以确定是在处理这个结构体的时候发生的问题

我们这里来梳理一下整个漏洞的原理以及修补方案，主要问题函数在dtls1_process_heartbeat 函数中，
首先通过 unsigned char p = &s->s3->rrec.data[0], pl; 这行代码来将心跳包的数据进行读取
然后通过 hbtype=*p++ 获取心跳包类型
通过 n2s(p, payload); 获取心跳包长度，并将长度放到 payload中

之后进行类型比较，如果数据包是TLS1_HB_REQUEST类型，则进行下面的流程

然后开辟空间，由于payload可以控制，则最大可以分配（1+2+65535+16）个字节的空间

然后开始在空间中添加类型，和，长度，并将原来的数据拷贝过去，这时便会发生信息泄露，由于拷贝的长度可以控制，当长度过大时候，便会导致读取pl中的数据，读取后

总结：在拷贝的时候，没有对数据和数据长度进行检查，导致，信息泄露

上一篇：Pwn with File结构体（一） 下一篇：HITCON 2017 Baby^...
1. 0 条回复
   - 动动手指，沙发就是你的了！