格 尔 软 件

安全漏洞“CVE-2014-0160”分析与评估报告

（2014.4.8）

1 CVE-2014-0160 漏洞描述

该漏洞在 OpenSSL 网站上的描述如下：

```
OpenSSL Security Advisory [07 Apr 2014]
=======================================

TLS heartbeat read overrun (CVE-2014-0160)
==========================================

A missing bounds check in the handling of the TLS heartbeat extension can be
used to reveal up to 64k of memory to a connected client or server.

Only 1.0.1 and 1.0.2-beta releases of OpenSSL are affected including
1.0.1f and 1.0.2-beta1.

Thanks for Neel Mehta of Google Security for discovering this bug and to
Adam Langley <agl@chromium.org> and Bodo Moeller <bmoeller@acm.org> for
preparing the fix.

Affected users should upgrade to OpenSSL 1.0.1g. Users unable to immediately
upgrade can alternatively recompile OpenSSL with -DOPENSSL_NO_HEARTBEATS.

1.0.2 will be fixed in 1.0.2-beta2.
```

该说明的大意是：在处理 TLS heartbeat 扩展项时，由于缺乏边界检查，导致可能将服务端最大 64K 的内存内容泄露给客户端，受影响的只有 1.0.1 系列和 1.0.2-beta 版。

2 CVE-2014-0160 漏洞分析

该漏洞源于 OpenSSL 代码中对 ClientHello 扩展项 Heartbeat 的处理，关于此扩展项的定义(详见 RFC6520)。

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

该漏洞对应的代码位于 OpenSSL 1.0.1 代码的 t1_lib.c 文件中：

```
#ifndef OPENSSL_NO_HEARTBEATS
int
tls1_process_heartbeat(SSL *s)
	{
	unsigned char *p = &s->s3->rrec.data[0], *pl;
	unsigned short hbtype;
	unsigned int payload;
	unsigned int padding = 16; /* Use minimum padding */

	/*
		漏洞分析：此处根据收到的数据包内容，解析得到心跳包长度 payload，
		但未判断此长度是否与实际收到的数据包长度相符，攻击者可能在此传递一个非法的长度。
	*/
	hbtype = *p++;
	n2s(p, payload);
	pl = p;

	if (s->msg_callback)
		s->msg_callback(0, s->version, TLS1_RT_HEARTBEAT,
			&s->s3->rrec.data[0], s->s3->rrec.length,
			s, s->msg_callback_arg);

	if (hbtype == TLS1_HB_REQUEST)
		{
		unsigned char *buffer, *bp;
		int r;

		/* Allocate memory for the response, size is 1 bytes
		 * message type, plus 2 bytes payload length, plus
		 * payload, plus padding
		 */
		buffer = OPENSSL_malloc(1 + 2 + payload + padding);
		bp = buffer;

		/* Enter response type, length and copy payload */
		*bp++ = TLS1_HB_RESPONSE;
		/*
			漏洞分析：如果使用之前解析得到的非法长度来进行 memcpy，
			就可能将当前进程内存堆中的其他数据复制到 pl 中，也即这个漏洞的可利用之处——
			可以获得服务端的部分内存数据。
		*/
		s2n(payload, bp);
		memcpy(bp, pl, payload);
		bp += payload;
		/* Random padding */
		RAND_pseudo_bytes(bp, padding);

		r = ssl3_write_bytes(s, TLS1_RT_HEARTBEAT, buffer, 3 + payload + padding);
```


上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

3 我们的结论

1. 该漏洞只影响 OpenSSL-1.0.1 – OpenSSL-1.0.1f 这部分版本，格尔软件的全线产品均未使用该版本的 OpenSSL 库，不受此漏洞影响。
2. 此漏洞受影响较大的主要是自行基于开源软件构建网站的互联网厂商。
3. 此漏洞给所有安全厂商都敲了警钟，协议实现的任何不完备之处，都可能被攻击者利用。

4 附录：目前已知的部分受影响厂商与产品

为方便客户进行安全评估，以下列出目前已知的部分受影响厂商与产品：

* cisco
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed

* F5
http://support.f5.com/kb/en-us/solutions/public/15000/100/sol15159.html?sr=36555669

* Juniper
http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10623

* vmware
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2076225

* citrix

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/

http://support.citrix.com/article/CTX140605

* Redhat

https://rhn.redhat.com/errata/RHSA-2014-0376.html

其他：

* Debian Wheezy (stable), OpenSSL 1.0.1e-2+deb7u4
* Ubuntu 12.04.4 LTS, OpenSSL 1.0.1-4ubuntu5.11
* CentOS 6.5, OpenSSL 1.0.1e-15
* Fedora 18, OpenSSL 1.0.1e-4
* OpenBSD 5.3 (OpenSSL 1.0.1c 10 May 2012) and 5.4 (OpenSSL 1.0.1c 10 May 2012)
* FreeBSD 10.0 - OpenSSL 1.0.1e 11 Feb 2013
* NetBSD 5.0.2 (OpenSSL 1.0.1e)
* OpenSUSE 12.2 (OpenSSL 1.0.1c)

上海格尔软件股份有限公司
上海市江场西路 299 弄 5 号（中铁中环时代广场 4 号楼）6 楼
http://www.koal.com/