OpenSSL Security Advisory [16 November 2010]

TLS extension parsing race condition.
=====================================

A flaw has been found in the OpenSSL TLS server extension code parsing which
on affected servers can be exploited in a buffer overrun attack.

The OpenSSL security team would like to thank Rob Hulswit for reporting this
issue.

The fix was developed by Dr Stephen Henson of the OpenSSL core team.

This vulnerability is tracked as CVE-2010-3864

Who is affected?
================

All versions of OpenSSL supporting TLS extensions contain this vulnerability
including OpenSSL 0.9.8f through 0.9.8o, 1.0.0, 1.0.0a releases.

Any OpenSSL based TLS server is vulnerable if it is multi-threaded and uses
OpenSSL's internal caching mechanism. Servers that are multi-process and/or
disable internal session caching are NOT affected.

In particular the Apache HTTP server (which never uses OpenSSL internal
caching) and Stunnel (which includes its own workaround) are NOT affected.

Recommendations for users of OpenSSL
====================================

Users of all OpenSSL 0.9.8 releases from 0.9.8f through 0.9.8o should update
to the OpenSSL 0.9.8p release which contains a patch to correct this issue.

Users of OpenSSL 1.0.0 and 1.0.0a should update to the OpenSSL 1.0.0b release
which contains a patch to correct this issue.

If upgrading is not immediately possible, the relevant source code patch
provided in this advisory should be applied.

Patch for OpenSSL 0.9.8 releases
================================

Index: ssl/t1_lib.c
===
RCS file: /v/openssl/cvs/openssl/ssl/t1_lib.c,v
retrieving revision 1.13.2.27
diff -u -r1.13.2.27 t1_lib.c
--- ssl/t1_lib.c   12 Jun 2010 13:18:58 -0000   1.13.2.27
+++ ssl/t1_lib.c   15 Nov 2010 15:20:14 -0000
@@ -432,14 +432,23 @@
                                switch (servname_type)
                                        {
                                case TLSEXT_NAMETYPE_host_name:
-                                       if (s->session->tlsext_hostname == NULL)
+   if (!s->hit)
+   {
-   if (len > TLSEXT_MAXLEN_host_name ||
-   ((s->session->tlsext_hostname

```
= OPENSSL_malloc(len+1)) == NULL))
+                                               if(s->session->tlsext_hostname)
+                                                       {
+                                                       *al = SSL_AD_DECODE_ERROR;
+                                                       return 0;
+                                                       }
+                                               if (len > TLSEXT_MAXLEN_host_name)
                                                        {
                                                        *al =
TLS1_AD_UNRECOGNIZED_NAME;

                                                        return 0;
                                                        }
+                                               if ((s->session->tlsext_hostname =
OPENSSL_malloc(len+1)) == NULL)
+                                                       {
+                                                       *al = TLS1_AD_INTERNAL_ERROR;
+                                                       return 0;
+                                                       }
                                                memcpy(s->session->tlsext_hostname,
sdata, len);
                                                s->session-
>tlsext_hostname[len]='\0';
                                                if (strlen(s->session-
>tlsext_hostname) != len) {
@@ -452,7 +461,8 @@

                                                }
                                        else
-                                               s->servername_done = strlen(s-
>session->tlsext_hostname) == len
+                                               s->servername_done = s->session-
>tlsext_hostname
+                                                       && strlen(s->session-
>tlsext_hostname) == len
                                                        && strncmp(s->session-
>tlsext_hostname, (char *)sdata, len) == 0;

                                        break;

Patch for OpenSSL 1.0.0 releases
================================

Index: ssl/t1_lib.c
===================================================================
RCS file: /v/openssl/cvs/openssl/ssl/t1_lib.c,v
retrieving revision 1.64.2.14
diff -u -r1.64.2.14 t1_lib.c
--- ssl/t1_lib.c        15 Jun 2010 17:25:15 -0000      1.64.2.14
+++ ssl/t1_lib.c        15 Nov 2010 15:26:19 -0000
@@ -714,14 +714,23 @@
                                switch (servname_type)
                                        {
                                case TLSEXT_NAMETYPE_host_name:
-                                       if (s->session->tlsext_hostname == NULL)
+                                       if (!s->hit)
                                                {
-                                               if (len > TLSEXT_MAXLEN_host_name ||
-                                                       ((s->session->tlsext_hostname
= OPENSSL_malloc(len+1)) == NULL))
+                                               if(s->session->tlsext_hostname)
```

```
+                                                       {
+                                                       *al = SSL_AD_DECODE_ERROR;
+                                                       return 0;
+                                                       }
+                                               if (len > TLSEXT_MAXLEN_host_name)
                                                        {
                                                        *al =
TLS1_AD_UNRECOGNIZED_NAME;
                                                        return 0;
                                                        }
+                                               if ((s->session->tlsext_hostname =
OPENSSL_malloc(len+1)) == NULL)
+                                                       {
+                                                       *al = TLS1_AD_INTERNAL_ERROR;
+                                                       return 0;
+                                                       }
                                                memcpy(s->session->tlsext_hostname,
sdata, len);
                                                s->session-
>tlsext_hostname[len]='\0';
                                                if (strlen(s->session-
>tlsext_hostname) != len) {
@@ -734,7 +743,8 @@

                                                }
                                        else
-                                               s->servername_done = strlen(s-
>session->tlsext_hostname) == len
+                                               s->servername_done = s->session-
>tlsext_hostname
+                                                       && strlen(s->session-
>tlsext_hostname) == len
                                                        && strncmp(s->session-
>tlsext_hostname, (char *)sdata, len) == 0;

                                        break;
@@ -765,15 +775,22 @@
                                *al = TLS1_AD_DECODE_ERROR;
                                return 0;
                                }
-                       s->session->tlsext_ecpointformatlist_length = 0;
-                       if (s->session->tlsext_ecpointformatlist != NULL)
OPENSSL_free(s->session->tlsext_ecpointformatlist);
-                       if ((s->session->tlsext_ecpointformatlist =
OPENSSL_malloc(ecpointformatlist_length)) == NULL)
+                       if (!s->hit)
                                {
-                               *al = TLS1_AD_INTERNAL_ERROR;
-                               return 0;
+                               if(s->session->tlsext_ecpointformatlist)
+                                       {
+                                       *al = TLS1_AD_DECODE_ERROR;
+                                       return 0;
+                                       }
+                               s->session->tlsext_ecpointformatlist_length = 0;
+                               if ((s->session->tlsext_ecpointformatlist =
OPENSSL_malloc(ecpointformatlist_length)) == NULL)
+                                       {
+                                       *al = TLS1_AD_INTERNAL_ERROR;
+                                       return 0;
```

```
+                                       }
+                               s->session->tlsext_ecpointformatlist_length =
ecpointformatlist_length;
+                               memcpy(s->session->tlsext_ecpointformatlist, sdata,
ecpointformatlist_length);
                                }
-                       s->session->tlsext_ecpointformatlist_length =
ecpointformatlist_length;
-                       memcpy(s->session->tlsext_ecpointformatlist, sdata,
ecpointformatlist_length);
 #if 0
                        fprintf(stderr,"ssl_parse_clienthello_tlsext s->session-
>tlsext_ecpointformatlist (length=%i) ", s->session-
>tlsext_ecpointformatlist_length);
                        sdata = s->session->tlsext_ecpointformatlist;
@@ -794,15 +811,22 @@
                                *al = TLS1_AD_DECODE_ERROR;
                                return 0;
                                }
-                       s->session->tlsext_ellipticcurvelist_length = 0;
-                       if (s->session->tlsext_ellipticcurvelist != NULL)
OPENSSL_free(s->session->tlsext_ellipticcurvelist);
-                       if ((s->session->tlsext_ellipticcurvelist =
OPENSSL_malloc(ellipticcurvelist_length)) == NULL)
+                       if (!s->hit)
                                {
-                               *al = TLS1_AD_INTERNAL_ERROR;
-                               return 0;
+                               if(s->session->tlsext_ellipticcurvelist)
+                                       {
+                                       *al = TLS1_AD_DECODE_ERROR;
+                                       return 0;
+                                       }
+                               s->session->tlsext_ellipticcurvelist_length = 0;
+                               if ((s->session->tlsext_ellipticcurvelist =
OPENSSL_malloc(ellipticcurvelist_length)) == NULL)
+                                       {
+                                       *al = TLS1_AD_INTERNAL_ERROR;
+                                       return 0;
+                                       }
+                               s->session->tlsext_ellipticcurvelist_length =
ellipticcurvelist_length;
+                               memcpy(s->session->tlsext_ellipticcurvelist, sdata,
ellipticcurvelist_length);
                                }
-                       s->session->tlsext_ellipticcurvelist_length =
ellipticcurvelist_length;
-                       memcpy(s->session->tlsext_ellipticcurvelist, sdata,
ellipticcurvelist_length);
 #if 0
                        fprintf(stderr,"ssl_parse_clienthello_tlsext s->session-
>tlsext_ellipticcurvelist (length=%i) ", s->session-
>tlsext_ellipticcurvelist_length);
                        sdata = s->session->tlsext_ellipticcurvelist;
```

References
==========

URL for this Security Advisory:

http://www.openssl.org/news/secadv_20101116.txt