

[UNIX] Apache mod_ssl Remote Buffer Overflow When Performing SSL Reverse Proxy

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-09/0032.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 09/14/04

To: list@securiteam.com

Date: 14 Sep 2004 18:16:47 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Apache mod_ssl Remote Buffer Overflow When Performing SSL Reverse Proxy

SUMMARY

mod_ssl has been found to be susceptible to a buffer overflow when performing an SSL reverse proxying.

DETAILS

Vulnerable Systems:

- * Apache with mod_ssl, version 2.0.50

Immune Systems:

- * Apache with mod_ssl, latest CVS (see below)

Intermittent segmentation faults occur in `char_buffer_read` at `ssl_engine_io.c:348` when using a `RewriteRule` to do reverse proxying to an SSL origin server running IIS. In order to reproduce this problem:

- * Set up an IIS server using SSL and running eRoom 6.

- * Add the following directives to `httpd.conf`:

```
Listen 47290
```

```
SSLProxyEngine on
```

```
RewriteEngine on
```

Securiteam: [UNIX] Apache mod_ssl Remote Buffer Overflow When Performing SSL Reverse Proxy

```
RewriteRule /(.*) https://some.eroom6.iis.server.com/\$1 [P]
```

* Visit a URL such as the following:

```
http://reverse.proxy.com:47290/eRoomASP/CookieTest.asp?facility=facility&URL=%2FeRoom%2FFacility%2FRoom
```

If this doesn't cause the segmentation fault immediately, clicking around for a while will eventually trigger it.

Note: Reverse proxying from non-SSL to SSL is not a good idea, but it keeps the example simpler.

A link to the bugzilla tracking system for Apache which describes the bug is provided for convenience:

```
<http://issues.apache.org/bugzilla/show\_bug.cgi?id=30134>
```

```
http://issues.apache.org/bugzilla/show\_bug.cgi?id=30134.
```

A log file of the error is listed below:

```
[Thu Jul 15 19:38:36 2004] [notice] child pid 42 exit signal Segmentation fault
```

```
(11), possible coredump in /usr/local/httpd-2.0.50
```

Build Date & Platform:

```
2004-07-14 build on SunOS 5.8 SUNW,UltraAX-i2
```

And a stack trace from gdb is also available:

```
#0 0xfef5060c in memcpy ()
  from /usr/platform/SUNW,UltraAX-i2/lib/libc_psr.so.1
#1 0xfeafef54 in char_buffer_read (buffer=0x1649ac,
  in=0x2000 <Address 0x2000 out of bounds>, inl=8192) at
ssl_engine_io.c:348
#2 0xfeaff388 in ssl_io_input_read (inctx=0x164990,
  buf=0x1649b8 "Content-Length:
121\r\nCort/Martonia/0_2615\r\nContent-Length:
121\r\nCent-Length: 121\r\nCmeport/Martonia/0_2615\r\nContent-Length:
121\r\nCmeport/Martonia/0_2615\r\nContent-Length:
121\r\nCrtonia/0_2615\r\nContent-Le"... , len=0xffbea8cc) at
ssl_engine_io.c:561
#3 0xfeaff624 in ssl_io_input_getline (inctx=0x164990,
  buf=0x1649b8 "Content-Length:
121\r\nCort/Martonia/0_2615\r\nContent-Length:
121\r\nCent-Length: 121\r\nCmeport/Martonia/0_2615\r\nContent-Length:
121\r\nCmeport/Martonia/0_2615\r\nContent-Length:
121\r\nCrtonia/0_2615\r\nContent-Le"... , len=0xffbea944) at
ssl_engine_io.c:712
#4 0xfeb00118 in ssl_io_filter_input (f=0x1669c0, bb=0x158f98,
  mode=4290685252, block=APR_BLOCK_READ, readbytes=0) at
ssl_engine_io.c:1226
#5 0x42978 in ap_get_brigade (next=0x1669c0, bb=0x158f98,
  mode=AP_MODE_GETLINE, block=APR_BLOCK_READ, readbytes=0)
  at util_filter.c:474
#6 0x4aab4 in net_time_filter (f=0x158e20, b=0x158f98,
```

Securiteam: [UNIX] Apache mod_ssl Remote Buffer Overflow When Performing SSL Reverse Proxy

```
mode=AP_MODE_GETLINE,
  block=APR_BLOCK_READ, readbytes=0) at core.c:3600
#7 0x42978 in ap_get_brigade (next=0x158e20, bb=0x158f98,
  mode=AP_MODE_GETLINE, block=APR_BLOCK_READ, readbytes=0)
  at util_filter.c:474
#8 0x43e0c in ap_rgetline_core (s=0xffbeab94, n=8192, read=0xffbeab90,
  r=0x1671b8, fold=1, bb=0x158f98) at protocol.c:214
#9 0x441a4 in ap_getline (s=0xffbeccd8 "Content-Length", n=8192,
r=0x1671b8,
  fold=1) at protocol.c:478
#10 0xfe8552d4 in ap_proxy_read_headers (r=0x1821d0, rr=0x1671b8,
  buffer=0xffbeccd8 "Content-Length", size=8192, c=0x1671b8)
  at proxy_util.c:457
#11 0xfe833014 in ap_proxy_http_process_response (p=0x157960, r=0x1821d0,
  p_conn=0x157ee8, origin=0x158168, backend=0x157f00, conf=0xf0268,
  bb=0x157e98, server_portstr=0xffbeed68 ":47290") at proxy_http.c:755
#12 0xfe833ba4 in ap_proxy_http_handler (r=0x1821d0, conf=0xf0268,
  url=0x158038
"/eRoomASP/CookieTest.asp?facility=memeport&URL=%2FeRoom%2Fmemeport%2FMartonia%2F0_2615",
proxyname=0x0, proxyport=60776) at proxy_http.c:1121
#13 0xfe85435c in proxy_run_scheme_handler (r=0x1821d0, conf=0xf0268,
  url=0x1839ce
"https://eromhost.aaa.bbb.com/eRoomASP/CookieTest.asp?facility=memeport&URL=%2FeRoom%2Fmemeport%2
proxyhost=0x0,
  proxyport=0) at mod_proxy.c:1113
#14 0xfe852ed8 in proxy_handler (r=0x1821d0) at mod_proxy.c:418
#15 0x359a8 in ap_run_handler (r=0x1821d0) at config.c:151
#16 0x35fa4 in ap_invoke_handler (r=0x1821d0) at config.c:358
#17 0x32c44 in ap_process_request (r=0x1821d0) at http_request.c:246
#18 0x2df14 in ap_process_http_connection (c=0x157a70) at http_core.c:250
#19 0x40090 in ap_run_process_connection (c=0x157a70) at connection.c:42
#20 0x403a4 in ap_process_connection (c=0x157a70, csd=0x157998)
  at connection.c:175
#21 0x3422c in child_main (child_num_arg=5) at prefork.c:609
#22 0x343ac in make_child (s=0x8edb0, slot=5) at prefork.c:703
#23 0x345fc in perform_idle_server_maintenance (p=0x8c690) at
prefork.c:838
#24 0x34a34 in ap_mpm_run (_pconf=0x0, plog=0x63400, s=0x83000)
  at prefork.c:1039
#25 0x3ad44 in main (argc=3, argv=0xffbef4ac) at main.c:617
```

Patch Availability:

The Apache development team have already fixed the bug and posted the fix to the CVS. The fix is available at

<http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.125&r2=1.126>
http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_io.c?r1=1.125&r2=1.126

ADDITIONAL INFORMATION

The information has been provided by <<mailto:jerome.athias@caramail.com>>
"JXrXme" ATHIAS.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.