

Re: OpenSSL buffer overflow

Source: <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2007-10/msg00016.html>

- *From:* Gregory Shapiro <gshapiro@xxxxxxxxxxx>
 - *Date:* Fri, 5 Oct 2007 09:35:23 -0700
-

Thanks! I did the same grep, but wasn't sure whether or not that particular function (SSL_get_shared_ciphers) got called by another function in OpenSSL which was originally called by some of the big apps like sendmail, apache and sshd

When I last researched this when the first problem with that function was announced, no other functions inside OpenSSL called it. That still appears to be the case:

```
/usr/src/crypto/openssl> grep -R SSL_get_shared_ciphers .  
./apps/s_client.c: p=SSL_get_shared_ciphers(s,buf,sizeof buf);  
./apps/s_server.c: if (SSL_get_shared_ciphers(con,buf,sizeof buf) != NULL)  
./apps/s_server.c: p=SSL_get_shared_ciphers(con,buf,bufsize);  
./doc/ssleay.txt:SSL_get_shared_ciphers  
./doc/ssl/ssl.pod:=item char *B<SSL_get_shared_ciphers>(SSL *ssl, char *buf, int len);  
./ssl/ssl.h:char * SSL_get_shared_ciphers(SSL *s, char *buf, int len);  
./ssl/ssl_lib.c:char *SSL_get_shared_ciphers(SSL *s,char *buf,int len)  
./util/ssleay.num:SSL_get_shared_ciphers 65 EXIST::FUNCTION:
```

Also, sendmail does not use it.

freebsd-security@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "freebsd-security-unsubscribe@xxxxxxxxxxx"