

Cipher Suite Mitigation for BEAST



PhoneFactor, Inc.
7301 West 129th Street
Overland Park, KS 66213
1-877-No-Token / 1-877-668-6536
www.phonefactor.com

Copyright © 2011 PhoneFactor, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of PhoneFactor, Inc., or its suppliers or affiliate companies.

Overview

The security protocols SSL 3.0 and TLS 1.0 are subject to an attack against CBC-based cipher suites (CVE-2011-3389). This attack, known as BEAST, is related to previous attacks against block ciphers in CBC mode, and affects AES and DES/3DES at all key lengths. While TLS 1.1 and 1.2 are not vulnerable, few deployed applications use these protocols.

As a workaround, PhoneFactor recommends increasing the priority of the RC4-based ciphersuites over the block-based ciphersuites, since RC4 does not use CBC. RC4 is widely supported by browsers and servers, and while it is not as cryptographically strong as AES, it is considerably stronger than AES_*_CBC and other block-based ciphersuites in light of this attack.

Instructions for making this change on IIS7-based servers are below. For Apache-based servers, it is sufficient to modify the SSLCipherSuites configuration directive to be something similar to the following: "!aNULL:!eNULL:!EXPORT:!DSS:!DES:!SSLv2:RC4-SHA:RC4-MD5:ALL" (Which means, roughly – disable all NULL ciphersuites, export suites, DSS, DES, and SSLv2 suites; Prefer RC4-SHA and RC4-MD5, then take whatever is left.) Please note that it is also necessary to turn on SSLHonorCipherOrder.

For example:

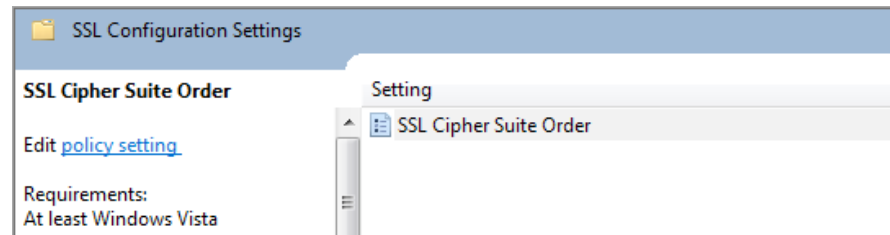
```
SSLHonorCipherOrder on
SSLCipherSuite !aNULL:!eNULL:!EXPORT:!DSS:!DES:RC4-SHA:RC4-MD5:ALL
```

These configuration settings are meant to be an example. They should work for most sites, but they may not be appropriate for sites that have special requirements. As always, use your own judgment and common sense. Test all changes thoroughly before putting them into production.

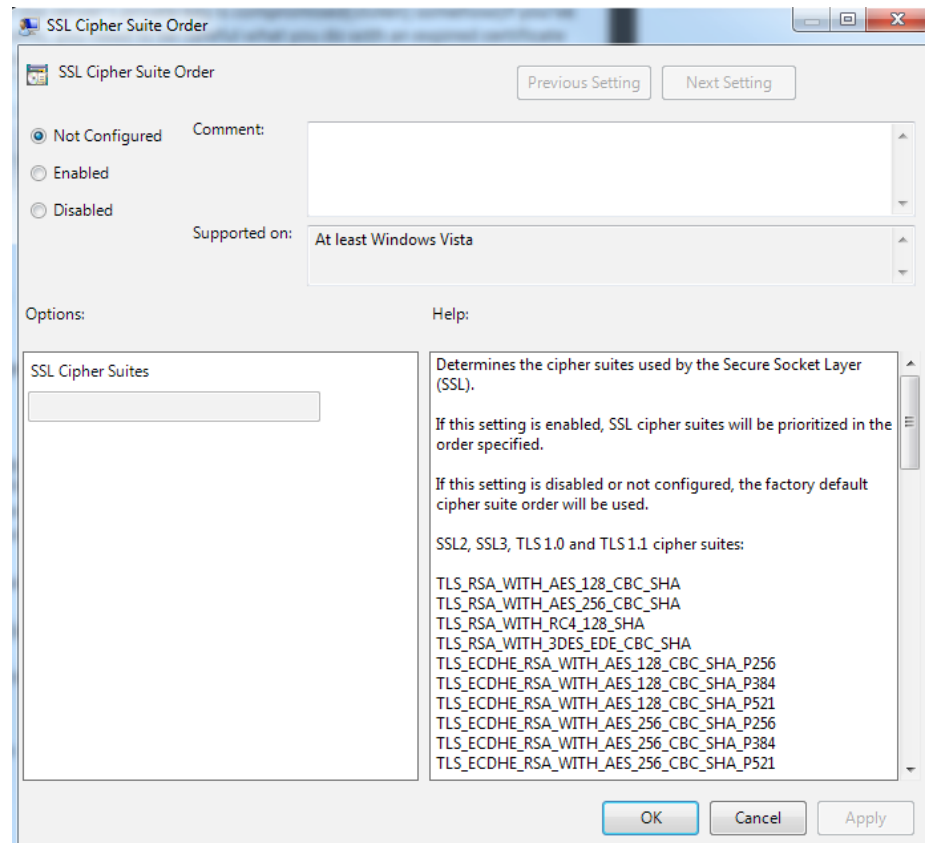
Mitigation

Open the *Local Group Policy Editor*.

1. At a command prompt, enter `gpedit.msc`. The Group Policy Object Editor appears.
2. Expand *Computer Configuration, Administrative Templates, Network*, and then click *SSL Configuration Settings*.
3. Under *SSL Configuration Settings*, double click the *SSL Cipher Suite Order* setting.

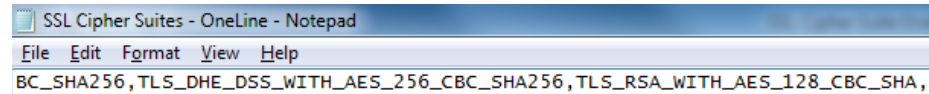


The window below will then be displayed.



The cipher suites TLS_RSA_WITH_RC4_128_SHA and TLS_RSA_WITH_RC4_128_MD5 must be put first on the line. The following procedure accomplishes this.

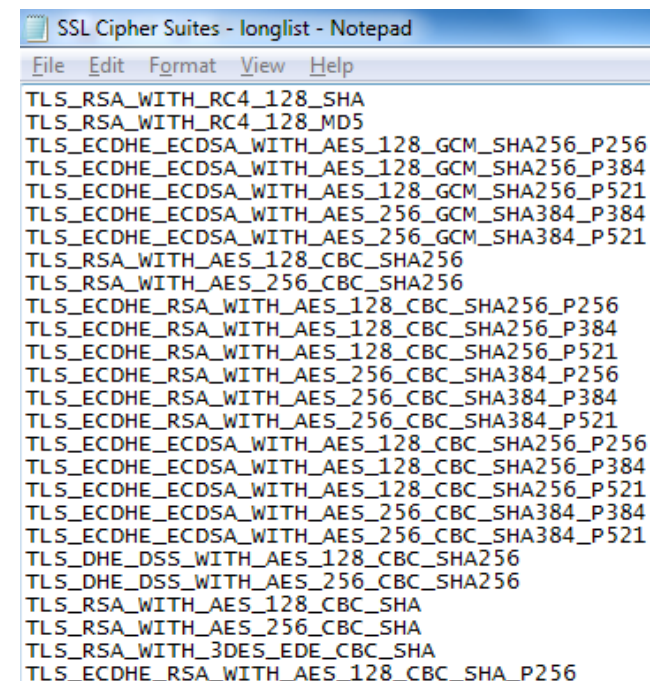
Open the .txt file that was accompanied with this document and copy the full line of text. **NOTE:** it is important that the text be all on one line, with no spaces, separated by commas, as in the image below:



```
SSL Cipher Suites - OneLine - Notepad
File Edit Format View Help
BC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,
```

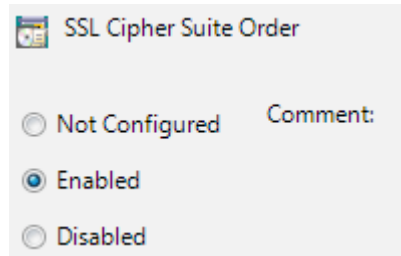
```
TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_WITH_RC4_128_MD5,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384,TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521,TLS_RSA_WITH_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_256_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384,TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P521,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384,TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P521,TLS_DHE_DSS_WITH_AES_128_CBC_SHA256,TLS_DHE_DSS_WITH_AES_256_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_3DES_EDE_CBC_SHA,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

For reference, this full list is what is included on the one line.



```
SSL Cipher Suites - longlist - Notepad
File Edit Format View Help
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P521
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P521
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P521
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384_P521
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P521
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384_P521
TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
```

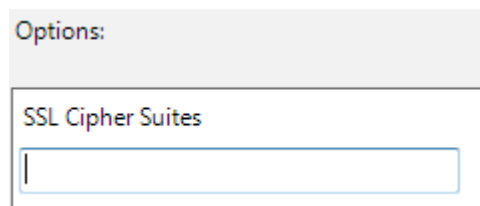
Back on the SSL *Cipher Suite Order*, click the radio button *Enabled*.



SSL Cipher Suite Order

Not Configured Comment:
 Enabled
 Disabled

Select the text box in the Options sections, below *SSL Cipher Suites*.

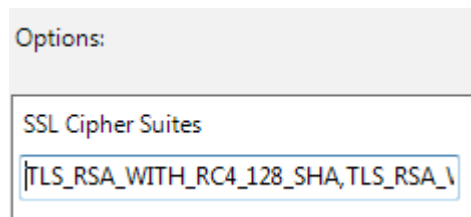


Options:

SSL Cipher Suites

|

Paste in this box.



Options:

SSL Cipher Suites

TLS_RSA_WITH_RC4_128_SHA,TLS_RSA_1

Click *OK*.

It is necessary to restart the computer after modifying this setting for the changes to take effect. SSL Cipher Suite Order Settings have been enabled and updated.

About PhoneFactor

PhoneFactor is the leading global provider of phone-based authentication. The company's award-winning platform is trusted by leading organizations to secure millions of logins and transactions each year. PhoneFactor provides strong, out-of-band security and is extremely user-friendly. It works with the customer's existing phone and can be used to secure online banking transactions, such as ACH, wire transfers, and payroll payments, as well as account logins. There are no devices to mail or certificates to install, so set up and deployment are quick and easy. No user training is required, and there is very little ongoing user support. PhoneFactor was recently named to the Bank Technology News FutureNow list of the top 10 technology innovators securing the banking industry today and a finalist in the SC Magazine Reader Trust Awards.

For more information, contact PhoneFactor at **877.No.Token (877.668.6536)** or visit our website at **www.phonefactor.com**.