

O CS permite algoritmos de criptografia forte para uma comunicação SSL

Índice

[Problema](#)

[Solução](#)

Problema

Àrevelia, o Cisco Security Manager (CS) apresenta as seguintes cifras para uma comunicação HTTPS:

```
%ASA-7-725011: Cipher[1] : AES128-SHA
%ASA-7-725011: Cipher[2] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[3] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725011: Cipher[5] : EDH-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[6] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[7] : DES-CBC-SHA
%ASA-7-725011: Cipher[8] : EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[9] : EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[10] : EXP-DES-CBC-SHA
%ASA-7-725011: Cipher[11] : EXP-EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[12] : EXP-EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[13] : ECDHE-ECDSA-AES128-SHA256
%ASA-7-725011: Cipher[14] : ECDHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[15] : AES128-SHA256
%ASA-7-725011: Cipher[16] : DHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[17] : DHE-DSS-AES128-SHA256
%ASA-7-725011: Cipher[18] : ECDHE-ECDSA-AES128-SHA
%ASA-7-725011: Cipher[19] : ECDHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[20] : AES128-SHA
%ASA-7-725011: Cipher[21] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[22] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[23] : ECDHE-ECDSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[24] : ECDHE-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[25] : DES-CBC3-SHA
%ASA-7-725011: Cipher[26] : EDH-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[27] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[28] : ADH-AES128-SHA256
%ASA-7-725011: Cipher[29] : ADH-AES128-SHA
%ASA-7-725011: Cipher[30] : ADH-DES-CBC3-SHA
%ASA-7-725011: Cipher[31] : DES-CBC-SHA
%ASA-7-725011: Cipher[32] : EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[33] : EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[34] : ADH-DES-CBC-SHA
%ASA-7-725011: Cipher[35] : EXP-DES-CBC-SHA
%ASA-7-725011: Cipher[36] : EXP-EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[37] : EXP-EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[38] : EXP-ADH-DES-CBC-SHA
%ASA-7-725011: Cipher[39] : NULL-SHA256
%ASA-7-725011: Cipher[40] : ECDHE-ECDSA-NULL-SHA
%ASA-7-725011: Cipher[41] : ECDHE-RSA-NULL-SHA
%ASA-7-725011: Cipher[42] : NULL-SHA
```

```
%ASA-7-725011: Cipher[43] : NULL-MD5
```

Contudo se nós configuramos o ASA para apoiar somente um algoritmo forte do encryptuon (como AES256-SHA):

A comunicação falhará e nós veremos o seguinte SYSLOG no ASA:

```
%ASA-7-725014: SSL lib error. Function: ssl3_get_client_hello Reason: no shared cipher
```

E o seguinte fazer logon o CS:

```
"Unable to communicate with the Device"  
The Security Manager Server and the device could not negotiate the security level"
```

Solução

Devido importar regulamentos em alguns países a aplicação do Oracle fornece um arquivo de política criptograficamente da jurisdição do padrão que limite a força dos algoritmos criptográficos. Se uns algoritmos mais fortes precisam de ser configurados ou estão configurados já no dispositivo (por exemplo, AES com chaves do 256-bit, grupo DH com 5,14,24), siga estas etapas:

1. Transfira os arquivos ilimitados da criptografia policy.jar da força das Javas 7 de <http://www.oracle.com>. [Cisco](http://www.oracle.com) recomenda procurar pelo seguinte no Web site do Oracle:

Javas ilimitadas 7 dos arquivos de política da jurisdição da força da extensão da criptografia das Javas (JCE)

<http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html>

2. Substitua local_policy.jar e US_export_policy.jar em seu server do gerenciador de segurança no dobrador CSCOpX \ CDM \ vms \ jre \ liberal \ Segurança.
3. Reinicie seu server do gerenciador de segurança.

Agora o CS apresentará as seguintes cifras:

```
%ASA-7-725011: Cipher[1] : AES128-SHA  
%ASA-7-725011: Cipher[2] : DHE-RSA-AES128-SHA  
%ASA-7-725011: Cipher[3] : DHE-DSS-AES128-SHA  
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA  
%ASA-7-725011: Cipher[5] : EDH-RSA-DES-CBC3-SHA  
%ASA-7-725011: Cipher[6] : EDH-DSS-DES-CBC3-SHA  
%ASA-7-725011: Cipher[7] : DES-CBC-SHA  
%ASA-7-725011: Cipher[8] : EDH-RSA-DES-CBC-SHA  
%ASA-7-725011: Cipher[9] : EDH-DSS-DES-CBC-SHA  
%ASA-7-725011: Cipher[10] : EXP-DES-CBC-SHA  
%ASA-7-725011: Cipher[11] : EXP-EDH-RSA-DES-CBC-SHA  
%ASA-7-725011: Cipher[12] : EXP-EDH-DSS-DES-CBC-SHA  
%ASA-7-725011: Cipher[13] : ECDHE-ECDSA-AES256-SHA384  
%ASA-7-725011: Cipher[14] : ECDHE-RSA-AES256-SHA384  
%ASA-7-725011: Cipher[15] : AES256-SHA256  
%ASA-7-725011: Cipher[16] : DHE-RSA-AES256-SHA256  
%ASA-7-725011: Cipher[17] : DHE-DSS-AES256-SHA256  
%ASA-7-725011: Cipher[18] : ECDHE-ECDSA-AES256-SHA  
%ASA-7-725011: Cipher[19] : ECDHE-RSA-AES256-SHA  
%ASA-7-725011: Cipher[20] : AES256-SHA
```

%ASA-7-725011: Cipher[21] : DHE-RSA-AES256-SHA
%ASA-7-725011: Cipher[22] : DHE-DSS-AES256-SHA
%ASA-7-725011: Cipher[23] : ECDHE-ECDSA-AES128-SHA256
%ASA-7-725011: Cipher[24] : ECDHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[25] : AES128-SHA256
%ASA-7-725011: Cipher[26] : DHE-RSA-AES128-SHA256
%ASA-7-725011: Cipher[27] : DHE-DSS-AES128-SHA256
%ASA-7-725011: Cipher[28] : ECDHE-ECDSA-AES128-SHA
%ASA-7-725011: Cipher[29] : ECDHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[30] : AES128-SHA
%ASA-7-725011: Cipher[31] : DHE-RSA-AES128-SHA
%ASA-7-725011: Cipher[32] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[33] : ECDHE-ECDSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[34] : ECDHE-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[35] : DES-CBC3-SHA
%ASA-7-725011: Cipher[36] : EDH-RSA-DES-CBC3-SHA
%ASA-7-725011: Cipher[37] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[38] : ADH-AES256-SHA256
%ASA-7-725011: Cipher[39] : ADH-AES256-SHA
%ASA-7-725011: Cipher[40] : ADH-AES128-SHA256
%ASA-7-725011: Cipher[41] : ADH-AES128-SHA
%ASA-7-725011: Cipher[42] : ADH-DES-CBC3-SHA
%ASA-7-725011: Cipher[43] : DES-CBC-SHA
%ASA-7-725011: Cipher[44] : EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[45] : EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[46] : ADH-DES-CBC-SHA
%ASA-7-725011: Cipher[47] : EXP-DES-CBC-SHA
%ASA-7-725011: Cipher[48] : EXP-EDH-RSA-DES-CBC-SHA
%ASA-7-725011: Cipher[49] : EXP-EDH-DSS-DES-CBC-SHA
%ASA-7-725011: Cipher[50] : EXP-ADH-DES-CBC-SHA
%ASA-7-725011: Cipher[51] : NULL-SHA256
%ASA-7-725011: Cipher[52] : ECDHE-ECDSA-NULL-SHA
%ASA-7-725011: Cipher[53] : ECDHE-RSA-NULL-SHA
%ASA-7-725011: Cipher[54] : NULL-SHA
%ASA-7-725011: Cipher[55] : NULL-MD5

E a conexão será agora bem sucedida:

%ASA-7-725012: Device chooses cipher AES256-SHA for the SSL session with client
asa:10.88.243.57/49949 to 10.122.160.233/443