CSM Abilita algoritmi di crittografia avanzata per la comunicazione SSL

Sommario

Problema

Per impostazione predefinita, Cisco Security Manager (CSM) presenta le seguenti cifrature per la comunicazione 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
```

Tuttavia, se l'ASA è configurata in modo da supportare solo un algoritmo di crittografia efficace (come AES256-SHA):

La comunicazione non riuscirà e sull'appliance ASA verrà visualizzato il seguente SYSLOG:

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

E il seguente accesso al CSM:

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

Soluzione

A causa delle normative di importazione in alcuni paesi, l'implementazione Oracle fornisce un file di criteri di giurisdizione di crittografia predefinito che limita la validità degli algoritmi di crittografia. Se è necessario configurare algoritmi più avanzati o se sono già configurati sul dispositivo (ad esempio, AES con chiavi a 256 bit, gruppo DH con 5,14,24), attenersi alla seguente procedura:

1. Scaricare i file Java 7 Unlimited Strength cryptography Policy.jar da http://www.oracle.com. Cisco consiglia di cercare quanto segue sul sito Web Oracle:

JCE (Java Cryptography Extension) File di criteri di validità illimitata Java 7

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

2. Sostituire local_policy.jar e US_export_policy.jar sul server Security Manager nella cartella CSCOpx\MDC\vms\jre\lib\security.
3. Riavviare il server Security Manager.

Ora il CSM presenterà i seguenti cifrari:

```
%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 la connessione avrà successo:

```
%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
```