CSM ermöglicht starke Verschlüsselungsalgorithmen für die SSL-Kommunikation

Inhalt

Problem

Standardmäßig stellt der Cisco Security Manager (CSM) die folgenden Verschlüsselungszeichen für die HTTPS-Kommunikation bereit:

```
%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
```

Wenn die ASA jedoch so konfiguriert wird, dass sie nur einen starken Verschlüsselungsalgorithmus unterstützt (z. B. AES256-SHA):

Die Kommunikation wird fehlschlagen, und es wird folgendes SYSLOG auf der ASA angezeigt:

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

Und die folgende Anmeldung auf dem CSM:

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

Lösung

Aufgrund von Importvorschriften in einigen Ländern bietet die Oracle-Implementierung eine Standard-Verschlüsselungs-Richtliniendatei, die die Stärke kryptografischer Algorithmen begrenzt. Wenn stärkere Algorithmen auf dem Gerät konfiguriert werden müssen oder bereits konfiguriert sind (z. B. AES mit 256-Bit-Schlüsseln, DH-Gruppe mit 5,14,24), gehen Sie wie folgt vor:

1. Laden Sie die Java 7-Dateien Unlimited Strength cryptography policy.jar von http://www.oracle.com herunter. Cisco empfiehlt, auf der Oracle-Website nach folgenden Informationen zu suchen:

Java Cryptography Extension (JCE) Unlimited Strength Jurisdiktion Richtliniendateien Java 7

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

2. Ersetzen Sie local_policy.jar und US_export_policy.jar auf Ihrem Security Manager-Server im Ordner CSCOpx\MDC\vms\jre\lib\security.
3. Starten Sie den Security Manager-Server neu.

Jetzt präsentiert der CSM die folgenden Verschlüsselungszeichen:

```
%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
```

Die Verbindung wird nun erfolgreich hergestellt:

```
%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
```