L'enregistrement de téléphone Exp-C/VCS-C bascule MRA avec les Certificats d'algorithme hachés par MD5

Contenu

Introduction

Ce document décrit un problème que vous pourriez rencontrer quand vous enregistrez votre téléphone au-dessus de mobile et l'Accès à distance (MRA) si le Message Digest 5 (MD5) hachait le certificat d'algorithme est utilisé, et il offre une solution au problème.

Problème

L'enregistrement de téléphone bascule MRA si le certificat utilisé sur l'autoroute-C/serveur de communication vidéo (VCS) - C sont générés avec l'utilisation de l'algorithme de signature de MD5.

Cause

L'utilisation de l'algorithme de hachage de MD5 dans les Certificats a pu permettre à un attaquant pour charrier le contenu, pour exécuter des attaques par phishing, ou pour exécuter des attaques homme-dans-le-moyennes. Microsoft a également libéré une année dernière consultative de Sécurité qui a limité l'utilisation des Certificats avec l'algorithme de hachage de MD5. Cette restriction est limitée aux Certificats délivrés sous des racines dans le programme de certificat racine de Microsoft : [Bulletin de renseignements de Sécurité de Microsoft : Mise à jour pour la condamnation de l'algorithme de hachage de MD5 pour le programme de certificat racine de](#)

Microsoft : Août 13, 2013

L'ID de bogue Cisco CSCuq95204 a été augmenté pour mettre à jour les documents VCS au déclarer que Cisco ne prend en charge pas des Certificats d'algorithme MD5-hashed.

Vérifiez la question

Détails de cette section comment vérifier si votre enregistrement échoue en raison de cette question.

Quand les tentatives de Jabber d'enregistrer un téléphone logiciel au-dessus de l'infrastrucure edge/MRA, l'enregistrement de téléphone logiciel de Jabber échoue si les ordinateurs d'autoroute utilisent le certificat MD5-hashed. Cependant, la nature de l'erreur varie et dépend de quel ordinateur utilise le certificat MD5-hashed.

Cas 1 : L'autoroute-C utilise le certificat MD5-Hashed et l'autoroute-e a un certificat avec un Secure Hash Algorithm (algorithme de SHA)

Vous rencontrez cette erreur dans les logs diagnostiques d'autoroute-C :

```
2014-09-20T06:06:43+05:30 Expressway-C UTCTime="2014-09-20 00:36:43,837" Module=
"developer.cvs.server" Level="INFO" CodeLocation="cvs(132)" Detail="Certificate
verification failure" SubjectCommonName="Expressway-E.edge.com" Error="(SEC_ERROR_
CERT_SIGNATURE_ALGORITHM_DISABLED) The certificate was signed using a signature
algorithm that is disabled because it is not secure."
```

Après cette erreur, un certificat "437 sans support » au message d'autoroute-e apparaît.

```
2014-09-20T06:06:43+05:30 Expressway-C tvcs: UTCTime="2014-09-20 00:36:43,840"
Module="network.sip" Level="DEBUG":  Action="Sent"  Local-ip="127.0.0.1"  Local-
port="22210"  Dst-ip="127.0.0.1"  Dst-port="25011"  Msg-Hash="5047300400093470988"
 SIPMSG:
 |SIP/2.0 437 Unsupported Certificate
 Via: SIP/2.0/TCP 127.0.0.1:5060;egress-zone=DefaultZone;branch=z9hG4bKeaaf784fd792
c156da3ff2b664a2eee751464.eb53ca5fcac328dc0f61631ec583fdf4;proxy-call-id=0e01fda1-
6704-4066-bcfd-06e2f3ded8f9;received=127.0.0.1;rport=25011
 Via: SIP/2.0/TLS 10.106.93.182:7001;egress-zone=TraversalserverzoneMRA;branch=z9hG
4bKc4ad3ddb1c5a24099882b10815ee247196.afc37861e975b930c7e624e1d5c6e967;proxy-call-id=
4436ec58-81a4-47a2-b4be-9f0b8b551209;received=10.106.93.182;rport=7001;ingress-zone=
TraversalclientzoneMRA;ingress-zone-id=1
 Via: SIP/2.0/TCP 127.0.0.1:5060;branch=z9hG4bKaa0592c35ecf47289c8efe37792f0c5095;
received=127.0.0.1;rport=25000;ingress-zone=DefaultZone
 Call-ID: 5050433d0d38b156@127.0.0.1
 CSeq: 35384 SERVICE
 From: <sip:serviceproxy@10.106.93.187>;tag=31976bf5fd009665
 To: <sip:serviceserver@10.106.93.187>;tag=f35f010a358ec6dd
 Server: TANDBERG/4130 (X8.2.1)
 Content-Length: 0
```

Cas 2 : L'autoroute-e utilise un certificat MD5-Hashed et l'autoroute-C a un certificat avec un algorithme de SHA

Vous rencontrez cette erreur dans les logs diagnostiques d'autoroute-e :

```
2014-11-28T20:17:38+05:30 Expressway-E UTCTime="2014-11-28 14:47:38,393" Module=
"developer.cvs.server" Level="INFO" CodeLocation="cvs(132)" Detail="Certificate
verification failure" SubjectCommonName="Expressway-C.edge.local" Error="(SEC_ERROR_
CERT_SIGNATURE_ALGORITHM_DISABLED) The certificate was signed using a signature
algorithm that is disabled because it is not secure."
```

Après cette erreur, le » message interdit par "403 pour jacasser le client apparaît.

```
2014-11-28T20:17:38+05:30 Expressway-E tvcs: UTCTime="2014-11-28 14:47:38,395"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="10.106.93.182" Local-
port="5061" Dst-ip="10.106.93.185" Dst-port="49174" Msg-Hash="8732905073947938174"
SIPMSG:
|SIP/2.0 403 Forbidden
Via: SIP/2.0/TLS 10.106.93.185:49174;branch=z9hG4bK00006db3;received=10.106.93.185
Call-ID: 005056ad-6bf90002-000038a2-00003b0a@10.106.93.185
CSeq: 104 REGISTER
From: <sip:8002@10.106.93.187>;tag=005056ad6bf9000200007e3c-000005e2
To: <sip:8002@10.106.93.187>;tag=baa86af3aca9e844
Server: TANDBERG/4130 (X8.2.1)
Content-Length: 0
```

Affaire 3 : Autoroute-e et autoroute-C les deux utilisation que les MD5-Hashed délivrent un certificat

Vous rencontrez cette erreur dans les logs diagnostiques d'autoroute-C :

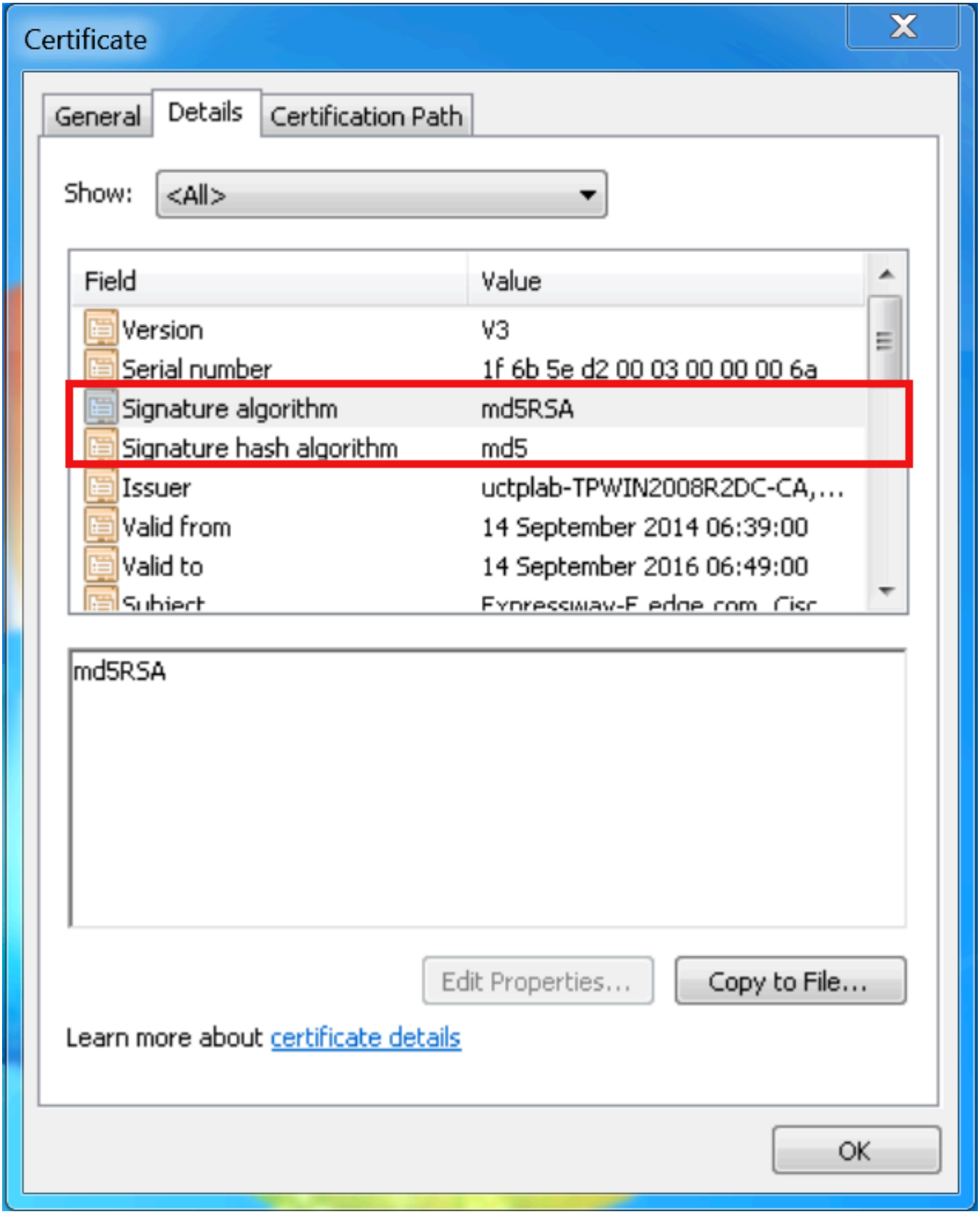
```
2014-11-28T20:50:44+05:30 Expressway-C UTCTime="2014-11-28 15:20:44,943" Module=
"developer.cvs.server" Level="INFO" CodeLocation="cvs(132)" Detail="Certificate
verification failure" SubjectCommonName="Expressway-E.edge.com" Error="(SEC_ERROR_
CERT_SIGNATURE_ALGORITHM_DISABLED) The certificate was signed using a signature
algorithm that is disabled because it is not secure."
```

Après cette erreur, le certificat "437 sans support » au message d'autoroute-e apparaît.

```
2014-11-28T20:50:44+05:30 Expressway-C tvcs: UTCTime="2014-11-28 15:20:44,945"
Module="network.sip" Level="DEBUG": Action="Sent" Local-ip="127.0.0.1" Local-
port="22210" Dst-ip="127.0.0.1" Dst-port="25753" Msg-Hash="136016498284976281"
SIPMSG:
|SIP/2.0 437 Unsupported Certificate
Via: SIP/2.0/TCP 127.0.0.1:5060;egress-zone=DefaultZone;branch=z9hG4bK22df47
ed2281a3bf3d88ece09bfbbc3a231977.0dbe343429e681275f6160e8c8af25fe;proxy-call-
id=2ee40ecc-4a1b-4073-87a6-07fbc3d7a6be;received=127.0.0.1;rport=25753
Via: SIP/2.0/TLS 10.106.93.182:7001;egress-zone=TraversalserverzoneMRA;branch=
z9hG4bK35a8b2cbb77db747c94e58bbf1d16cf1108.1c42f037f9ac98c59766cb84d0d3af10;
proxy-call-id=a8938902-2e0c-4a49-b900-a3b631920553;received=10.106.93.182;rport=
7001;ingress-zone=TraversalclientzoneMRA;ingress-zone-id=1
Via: SIP/2.0/TCP 127.0.0.1:5060;branch=z9hG4bKb2da522d9f1b5ad1bc2f415f5f01d0d2107;
received=127.0.0.1;rport=25000;ingress-zone=DefaultZone
Call-ID: 019ed17f1344e908@127.0.0.1
CSeq: 54313 SERVICE
From: <sip:serviceproxy@10.106.93.187>;tag=3426bb81de53e3b6
To: <sip:serviceserver@10.106.93.187>;tag=2128ce8a1f90cb7b
Server: TANDBERG/4130 (X8.2.1)
Content-Length: 0
```

Vérifiez l'algorithme de certificat

Ce tir d'écran affiche comment vérifier l'algorithme de certificat qui est utilisé.



Solution

Normalement l'Autorité de certification (CA) ne fournit plus à des Certificats l'algorithme de MD5. Mais parfois les clients utilisent une approche mélangée où le certificat sur l'autoroute-C est généré avec leur entreprise Microsoft CA et autoroute-e utilise un certificat délivré par un public

CA tel que GoDaddy.

Si la racine CA de Microsoft d'entreprise utilise l'algorithme de MD5, alors cette question se produit. Vous pouvez modifier la racine CA afin d'utiliser l'algorithme SHA1 si vous avez des services CA ce passage sur la Microsoft Windows Server 2008. Référez-vous au est il possible de changer l'algorithme de hachage quand je renouvelle l'article de la racine CA afin de modifier l'algorithme de hachage.