Переключения при отказе Регистрации телефона Exp-C/VCS-C MRA с MD5 Хешированные Сертификаты Алгоритма

Содержание

Введение

Этот документ описывает проблему, с которой вы могли бы встретиться при регистрации телефона по Мобильному и Удаленному доступу (MRA), если хешированный сертификат алгоритма алгоритма представления сообщения в краткой форме 5 (MD5) используется, и это предлагает решение проблемы.

Проблема

Если сертификат, используемый на Сервере подключения Expressway-C/Video (VCS)-C, генерируется с использованием алгоритма сигнатуры MD5, регистрация телефона переключается при отказе MRA.

Причина

Использование алгоритма хэширования MD5 в сертификатах могло позволить атакующему имитировать содержание, выполнять фишинговые атаки или выполнять атаки по перехвату и возможному изменению передаваемых данных. Microsoft также освободила рекомендацию по вопросам безопасности в прошлом году, которая ограничила использование сертификатов с алгоритмом хэширования MD5. Это ограничение ограничено

сертификатами, выполненными под root в программе корневого сертификата Microsoft: Консультативная Защита Microsoft: Обновление для осуждения алгоритма хеширования MD5 для программы корневого сертификата Microsoft: 13 августа 2013

CSCuq95204 идентификатора ошибки Cisco был повышен для обновления документов VCS, чтобы сообщить, что Cisco не поддерживает хешированные MD5 сертификаты алгоритма.

Проверьте проблему

Этот раздел детализирует, как проверить, отказывает ли ваша регистрация из-за этой проблемы.

Если машины Скоростной автомагистрали используют хешированный MD5 сертификат, когда Jabber пытается зарегистрировать программный телефон по edge/MRA infrastrucure, регистрационные сбои программного телефона Jabber. Однако природа ошибки варьируется и зависит, на котором машина использует хешированный MD5 сертификат.

Пример 1: Скоростная-автомагистраль-C использует Хешированный MD5 сертификат, и скоростная-автомагистраль-E имеет сертификат с защищенным алгоритмом хэширования (алгоритм SHA)

Вы встречаетесь с этой ошибкой в журналах диагностики Скоростной-автомагистрали-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."
```

После этой ошибки появляются "437 неподдерживаемых сертификатов" к сообщению Скоростной-автомагистрали-E.

```
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
```

Случай 2: Скоростная-автомагистраль-E использует Хешированный MD5

сертификат, и скоростная-автомагистраль-C имеет сертификат с алгоритмом SHA

Вы встречаетесь с этой ошибкой в журналах диагностики Скоростной-автомагистрали-E:

```
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
```

После этой ошибки "403 Запрещенных" сообщения для Передачи бессмысленных данных появляется клиент.

```
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
```

Случай 3: Скоростная-автомагистраль-E и скоростная-автомагистраль-C оба используют Хешированный MD5 сертификат

Вы встречаетесь с этой ошибкой в журналах диагностики Скоростной-автомагистрали-C:

```
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
```

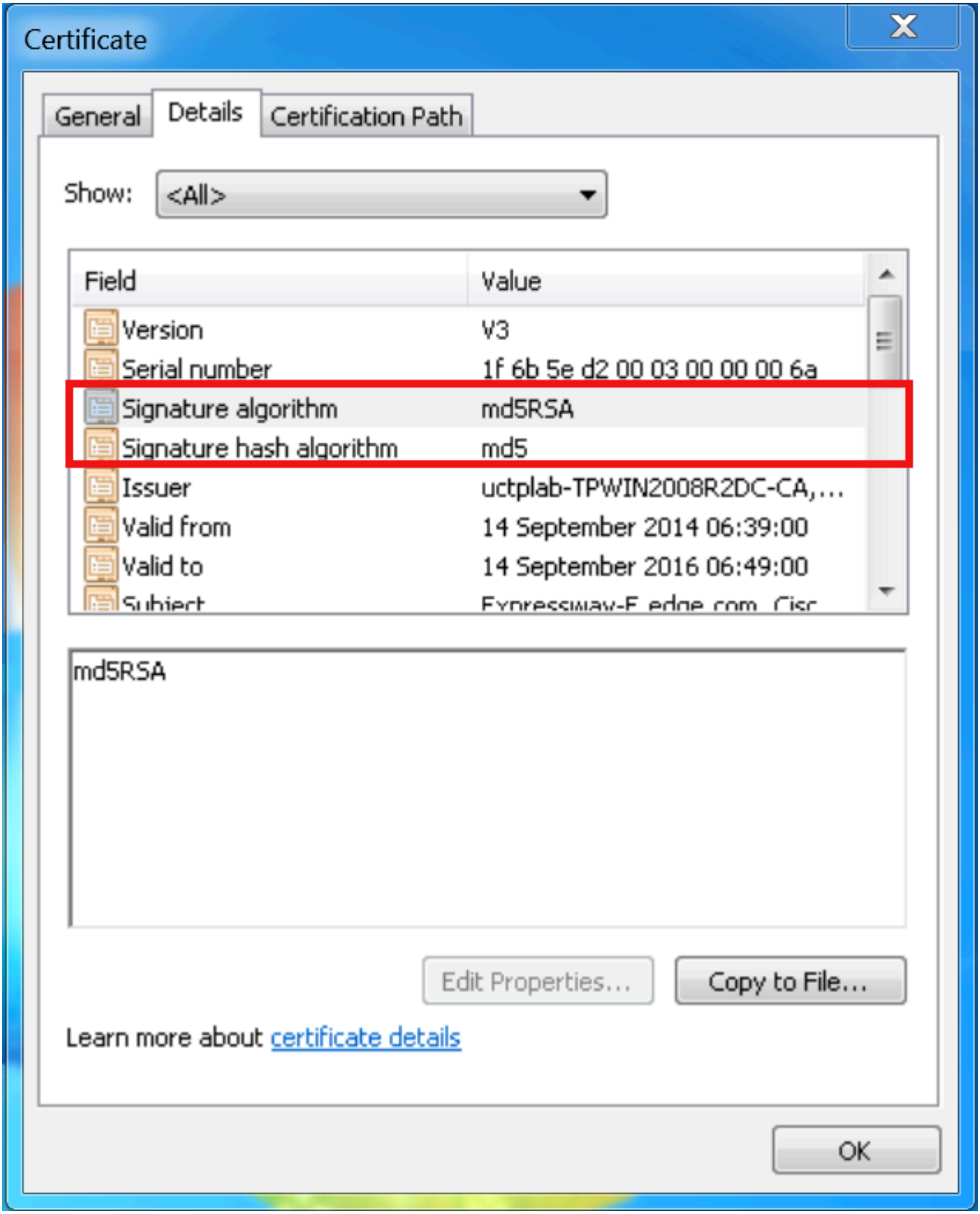
После этой ошибки появляются "437 неподдерживаемых сертификатов" к сообщению

Скоростной-автомагистрали-E.

```
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
```

Проверьте алгоритм сертификата

Этот снимок экрана показывает, как проверить алгоритм сертификата, который используется.



Решение

Обычно Центр сертификации (CA) не предоставляет сертификатам алгоритм MD5 больше. Но иногда клиенты используют смешанный подход в чем, сертификат на Скоростной-автомагистрали-C генерируется с их Предприятием Microsoft CA, и Скоростная-

автомагистраль-E использует сертификат, выполненный общественностью CA, такой как GoDaddy.

Если Узел CA Предприятия Microsoft использует алгоритм MD5, то эта проблема происходит. Можно модифицировать узел CA для использования алгоритма SHA1, если у вас есть сервисы CA, которые работают на Microsoft Windows server 2008. См. этого возможный изменить алгоритм хэширования, когда я возобновляю статью Root CA для изменения алгоритма хеширования.