

El registro de teléfono Exp-C/VCS-C falla sobre MRA con los Certificados desmenuzados MD5 del algoritmo

Contenido

[Introducción](#)

[Problema](#)

[Causa](#)

[Verifique el problema](#)

[Caso 1: La autopista-C utiliza el certificado MD5-Hashed y la autopista-e tiene un certificado con un algoritmo de troceo seguro \(algoritmo SHA\)](#)

[Caso 2: La autopista-e utiliza un certificado MD5-Hashed y la autopista-C tiene un certificado con un algoritmo SHA](#)

[Caso 3: La autopista-e y la autopista-C ambas utilizan el certificado MD5-Hashed](#)

[Verifique el algoritmo del certificado](#)

[Solución](#)

Introducción

Este documento describe un problema que usted puede ser que encuentre cuando usted registra su teléfono sobre el móvil y el Acceso Remoto (MRA) si se utiliza el certificado desmenuzado del algoritmo de la publicación de mensaje 5 (MD5), y ofrece una solución al problema.

Problema

El registro de teléfono falla sobre MRA si el certificado usado en la autopista-C/el servidor del comunicación mediante video (VCS) - C se genera con el uso del algoritmo de la firma MD5.

Causa

El uso del algoritmo de troceo MD5 en los Certificados podía permitir un atacante al contenido del spoof, realizar los ataques del phishing, o realizar los ataques del intermediario. Microsoft también liberó un Security Advisory el año pasado que restringió el uso de los Certificados con el algoritmo de troceo MD5. Esta restricción se limita a los Certificados publicados bajo raíces en el programa del certificado raíz de Microsoft: [Security Advisory de Microsoft: Actualización para la deprecación del algoritmo de troceo MD5 para el programa del certificado raíz de Microsoft: De agosto el 13 de 2013](#)

El Id. de bug Cisco [CSCuq95204](#) se ha aumentado para poner al día los documentos VCS al

estado que Cisco no soporta los Certificados del algoritmo MD5-hashed.

Verifique el problema

Detalles de esta sección cómo verificar si su registro falla debido a este problema.

Cuando el Jabber intenta registrar un Soft Phone sobre el infraestructure edge/MRA, el registro del Soft Phone del Jabber falla si las máquinas de la autopista utilizan el certificado MD5-hashed. Sin embargo, la naturaleza del error varía y depende de qué máquina utiliza el certificado MD5-hashed.

Caso 1: La autopista-C utiliza el certificado MD5-Hashed y la autopista-e tiene un certificado con un algoritmo de troceo seguro (algoritmo SHA)

Usted encuentra este error en los registros de diagnóstico de la autopista-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."
```

Después de este error, un certificado sin apoyo "437" al mensaje de la autopista-e aparece.

```
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="504730040093470988" SIPMSG:  
|SIP/2.0 437 Unsupported Certificate  
Via: SIP/2.0/TCP 127.0.0.1:5060;egress-zone=DefaultZone;branch=z9hG4bKeaaf784fd792c156da3ff2b664a2eee751464.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=z9hG4bKc4ad3ddb1c5a24099882b10815ee247196.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
```

Caso 2: La autopista-e utiliza un certificado MD5-Hashed y la autopista-C tiene un certificado con un algoritmo SHA

Usted encuentra este error en los registros de diagnóstico de la autopista-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="504730040093470988" SIPMSG:  
|SIP/2.0 437 Unsupported Certificate
```

Via: SIP/2.0/TCP 127.0.0.1:5060;egress-zone=DefaultZone;branch=z9hG4bKeaaf784fd792c156da3ff2b664a2eee751464.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=z9hG4bKc4ad3ddb1c5a24099882b10815ee247196.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

Después de este error, el mensaje prohibido "403 para farfullar al cliente aparece.

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

Caso 3: La autopista-e y la autopista-C ambas utilizan el certificado MD5-Hashed

Usted encuentra este error en los registros de diagnóstico de la autopista-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

Después de este error, el certificado sin apoyo "437" al mensaje de la autopista-e aparece.

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=z9hG4bK22df47ed2281a3bf3d88ece09bfbbc3a231977.0dbe343429e681275f6160e8c8af25fe;proxy-call-id=2ee40ecc-4a1b-4073-87a6-07fbc3d7a6be;received=127.0.0.1;rport=25753

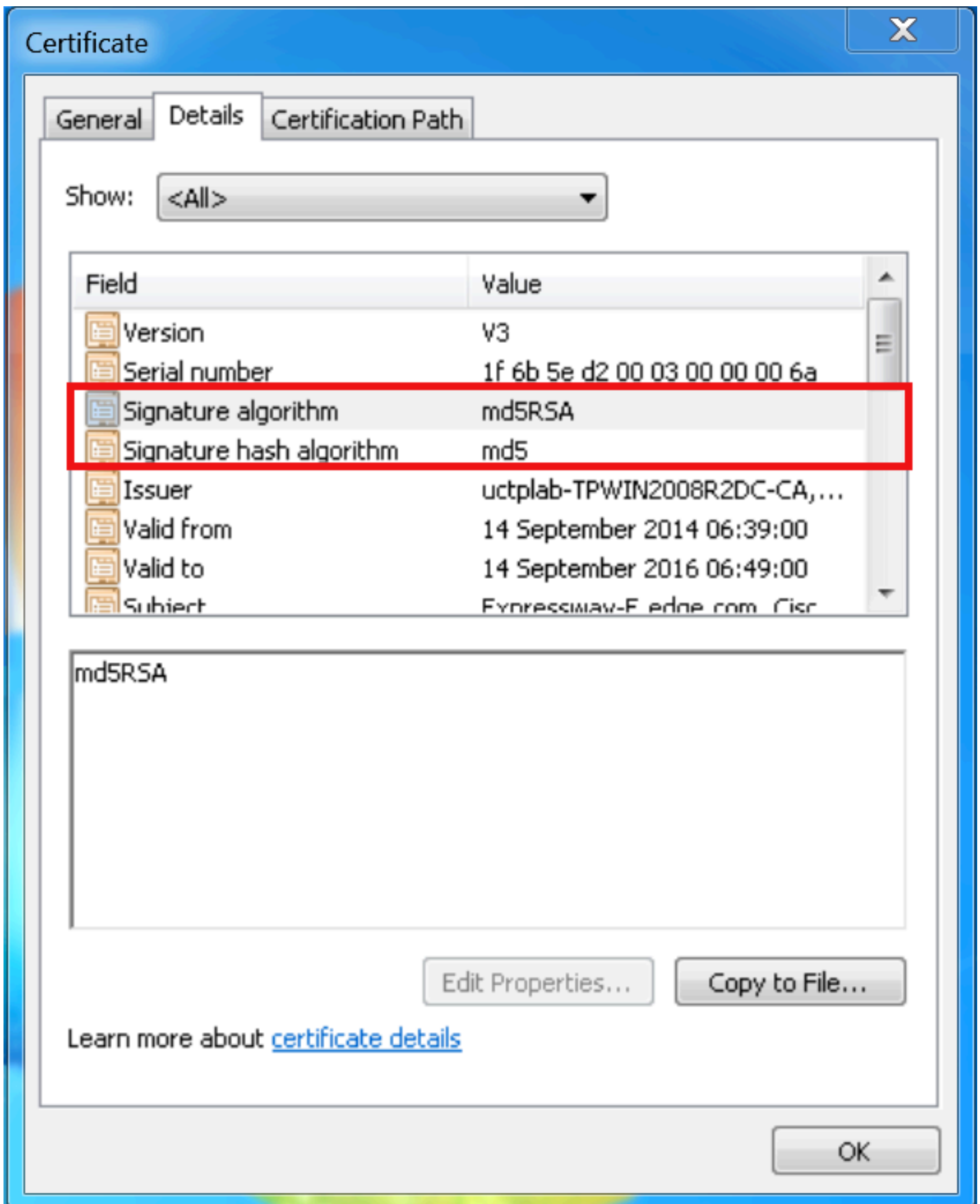
Via: SIP/2.0/TLS 10.106.93.182:7001;egress-zone=TraversalserverzoneMRA;branch=z9hG4bK35a8b2cbb77db747c94e58bbf1d16cf1108.1c42f037f9ac98c59766cb84d0d3af10;proxy-call-id=a8938902-2e0c-4a49-b900-a3b631920553;received=10.106.93.182;rport=7001;ingress-zone=TraversalclientzoneMRA;ingress-zone-id=1

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

Verifique el algoritmo del certificado

Este tiro de pantalla muestra cómo verificar el algoritmo del certificado se utiliza que.



Solución

El Certificate Authority (CA) no proporciona normalmente los Certificados con el algoritmo MD5 más. Pero los clientes utilizan a veces un acercamiento mezclado en donde el certificado en la autopista-C se genera con su empresa Microsoft CA y la autopista-e utiliza un certificado

publicado por CA público tal como GoDaddy.

Si la empresa Microsoft raíz CA utiliza el algoritmo MD5, después este problema ocurre. Usted puede modificarse raíz CA para utilizar el algoritmo SHA1 si usted tiene los servicios de CA que funcionan con en el Microsoft Windows server 2008. Refiera a [es él posible cambiar el algoritmo de troceo cuando renuevo raíz CA el](#) artículo para modificar el algoritmo de troceo.