O registro do telefone Exp-C/VCS-C falha sobre MRA com os Certificados picados MD5 do algoritmo

Índice

Introdução

Este documento descreve um problema que você pôde encontrar quando você registra seu telefone sobre o móbil e o Acesso remoto (MRA) se o certificado picado do algoritmo do message digest 5 (MD5) é usado, e oferece uma solução ao problema.

Problema

O registro do telefone falha sobre MRA se o certificado usado na via expressa-C/server de comunicação de vídeo (VC) - C é gerado com o uso do algoritmo da assinatura MD5.

Causa

O uso do algoritmo de hash MD5 nos Certificados podia permitir um atacante ao índice do spoof, executar ataques do phishing, ou executar ataques que envolva pessoas. Microsoft igualmente liberou uma Recomendação de Segurança no ano passado que restringisse o uso dos Certificados com o algoritmo de hash MD5. Esta limitação é limitada aos Certificados emitidos sob raizes no programa do certificado de raiz de Microsoft: Recomendação de Segurança de Microsoft: Atualização para o deprecation do algoritmo de hashing MD5 para o programa do certificado de raiz de Microsoft: agosto 13, 2013

A identificação de bug Cisco CSCuq95204 foi aumentada para atualizar os documentos VC ao

estado que Cisco não apoia Certificados do algoritmo MD5-hashed.

Verifique a edição

Detalhes desta seção como verificar se seu registro falha devido a esta edição.

Quando o Jabber tenta registrar um telefone de software sobre o infrastrucure edge/MRA, o registro do telefone de software do Jabber falha se as máquinas da via expressa usam o certificado MD5-hashed. Contudo, a natureza do erro varia e depende de que máquina usa o certificado MD5-hashed.

Caso 1: A via expressa-C usa o certificado MD5-Hashed e a via expressa-e tem um certificado com um algoritmo de mistura segura (algoritmo SHA)

Você encontra este erro nos log de diagnóstico da via expressa-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."
```

Após este erro, um certificado "437 unsupported" à mensagem da via expressa-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="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
```

Caso 2: A via expressa-e usa um certificado MD5-Hashed e a via expressa-C tem um certificado com um algoritmo SHA

Você encontra este erro nos log de diagnóstico da via expressa-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."
```

Após este erro, a” mensagem proibida "403 para jabber o 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: A via expressa-e e a via expressa-C ambos usam o certificado MD5-Hashed

Você encontra este erro nos log de diagnóstico da via expressa-C:

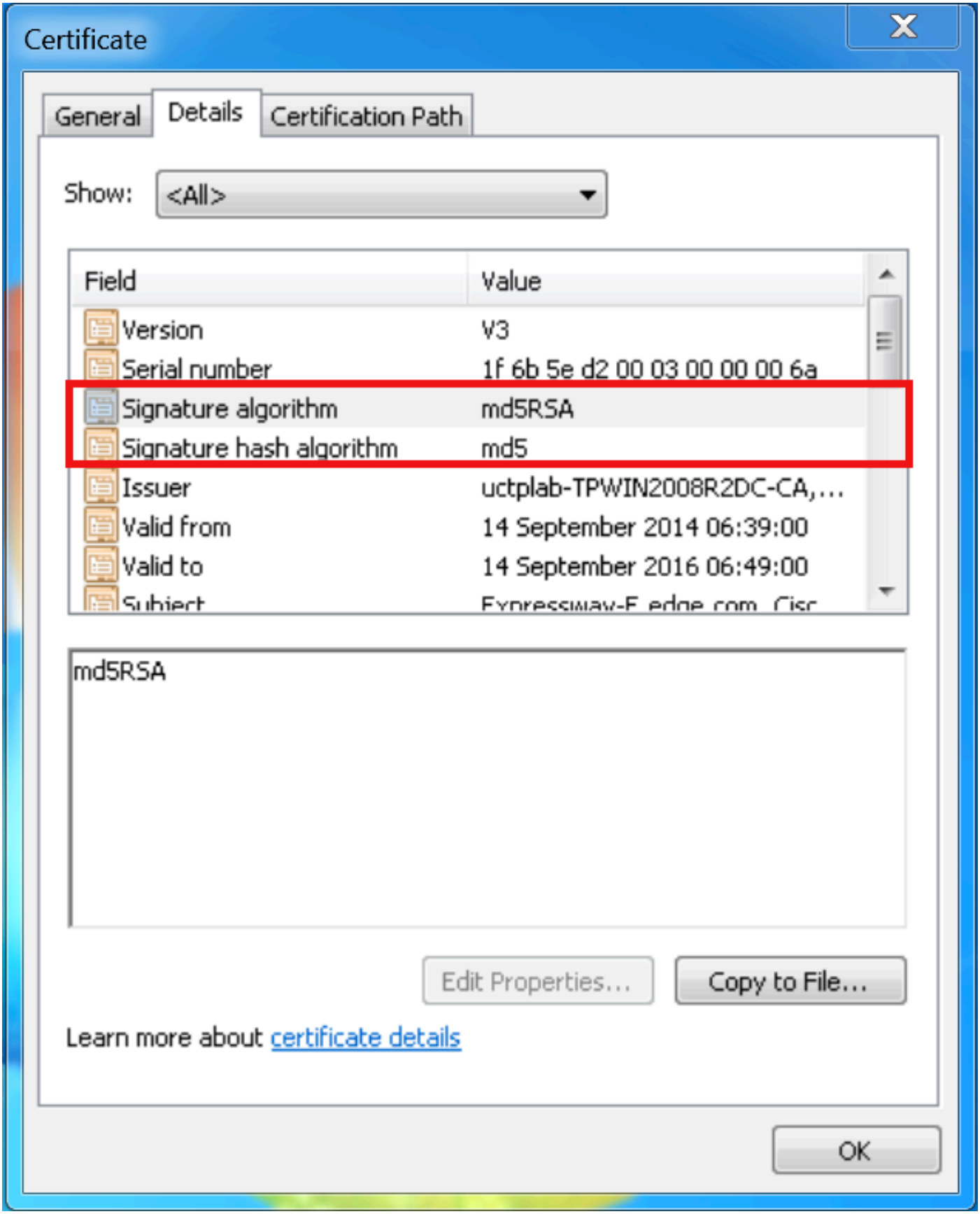
```
2014-11-28T20:50:44+05:30 Expressway-C UTCTime="2014-11-28 15:20:44,943" Module=
"developer.cvs.server" Level="INFO" CodeLocation="cvs(132)" Detail="Certificate
verification failure" SubjectCommonName="Expressway-E.edge.com" Error="(SEC_ERROR_
CERT_SIGNATURE_ALGORITHM_DISABLED) The certificate was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

Após este erro, o certificado "437 unsupported” à mensagem da via expressa-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=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
```

Verifique o algoritmo do certificado

Este tiro de tela mostra como verificar o algoritmo do certificado que é usado.



Solução

Normalmente o Certificate Authority (CA) não fornece Certificados o algoritmo MD5 anymore. Mas às vezes os clientes usam uma aproximação misturada onde o certificado na via expressa-C é gerado com sua empresa Microsoft CA e a via expressa-e usa um certificado emitido por CA

público tal como GoDaddy.

Se a CA raiz de Microsoft da empresa usa o algoritmo MD5, a seguir esta edição ocorre. Você pode alterar a CA raiz a fim usar o algoritmo SHA1 se você tem os serviços de CA que executam no Microsoft Windows server 2008. Refira é ele possível mudar o algoritmo de hash quando eu renovo o artigo da CA raiz a fim alterar o algoritmo de hashing.