EXPC/VCS C电话注册故障切换与MD5被切细的算法证书的MRA

目录

简介

本文描述您也许遇到的问题，当您注册您的在莫比尔和远程访问(MRA)时的电话，如果使用消息摘要5 (MD5)被切细的算法证书，并且提供解决方案对问题。

问题

电话注册故障切换MRA，如果在ExpresswayC使用的证书/视频通信服务器(VCS) - C生成与使用MD5签名算法。

原因

使用在证书的MD5散列算法能允许攻击者伪装内容，进行网络钓鱼攻击或者进行中间人攻击。 Microsoft去年也发布限制使用证书与MD5散列算法的安全建议。 此限制对证书被限制发出在Microsoft根证明程序的根下：[Microsoft安全建议：为MD5散列算法的反对的更新Microsoft根证明程序的：奥古斯特13， 2013](#)

Cisco Bug ID [CSCuq95204](#)被上升更新VCS文档到阐明， Cisco不支持MD5-hashed算法证书。

验证问题

此部分详细信息如何验证因此，如果您的注册发生故障问题。

当Jabber尝试注册在edge/MRA infrastrucure时的一个软电话， Jabber软电话注册发生故障，如果Expressway机器使用MD5-hashed证书。然而，错误的本质变化并且依靠哪计算机使用MD5-hashed证书。

第 1 种情况：ExpresswayC使用MD5-hashed证书，并且ExpresswayE有与安全散列算法(SHA算法)的一证书

您遇到在ExpresswayC诊断记录的此错误：

```
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."
```

在此错误以后，一"437不支持的证书”对ExpresswayE消息出现。

```
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
```

第 2 种情况：ExpresswayE使用一MD5-hashed证书，并且ExpresswayC有与SHA算法的一证书

您遇到在ExpresswayE诊断记录的此错误：

```
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
```

在此错误以后，闲聊客户端的"403禁止的”消息出现。

```
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
```

实例3：其它WRR加权修改ExpresswayE和ExpresswayC两个使用MD5-hashed证书

您遇到在ExpresswayC诊断记录的此错误：

```
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
```

在此错误以后， "437不支持的证书”对ExpresswayE消息出现。

```
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
```

验证证书算法

此屏幕画面显示如何验证使用的证书算法。

解决方案

通常Certificate Authority (CA)不再提供证书MD5算法。但是客户有时使用一混合方法，在ExpresswayC的证书生成与他们的企业Microsoft CA和ExpresswayE使用公共CA发出的证书例如GoDaddy。

如果企业Microsoft根CA使用MD5算法，则此问题出现。您能修改根CA为了使用SHA1算法，如果有在MS Windows服务器运行2008年的CA服务。 当我更新根CA条款为了修改哈希算法时，参考是它可能更改散列算法。