9.5和电子邮件安全性升级的更新的AsyncOS与出故障的更旧的证书(MD5)通信TLSv1.2

Contents

[Introduction](#)
[传统证书(MD5)在9.5 AsyncOS造成TLSv1.2通信失效电子邮件安全性升级的和更新](#)
[纠正措施](#)
[CLI纠正措施(如果GUI不可能被获取)](#)
[Related Information](#)
[相关的思科支持社区讨论](#)

Introduction

本文描述将适用的必要的步骤，如果遇到TLS通信的一个问题或者访问Web接口，在升级到电子邮件安全版本9.5或以上的AsyncOS以后在Cisco电子邮件安全工具(ESA)上。

传统证书(MD5)在9.5 AsyncOS造成TLSv1.2通信失效电子邮件安全性升级的和更新

> **Note**:下列是在工具上应用的当前证书示例的一个列出的解决方法。然而，下面的步骤可能工具也适用于所有MD5签名的证书。

当执行对AsyncOS的升级后电子邮件安全版本9.5和以上的，其中任一个传统IronPort证书示例在使用中和应用为发运，接受或LDAP，可能经历错误，当设法通过TLSv1/TLSv1.2沟通与一些域时。 TLS错误将引起所有入站或呼出会话发生故障。

如果证书被应用于HTTPS接口，现代Web浏览器不能访问工具的Web接口。

邮件日志应该看起来类似于以下示例：

```
Tue Jun 30 15:27:59 2015 Info: ICID 4420993 TLS failed: (336109761,
'error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
```

此错误是由签名算法造成的被运用于是更旧的认证MD5;然而，与连接工具/浏览器产生关联的证书只支持SHA签名基于算法。虽然，有的更旧的证书示例MD5签名是在工具上同一时间新的SHA基于证书示例上述错误只将表明自己，如果MD5签名基于认证被应用于指定的部分(即接受，发运等等)

下面从除新的证书示例工具的cli拉的示例(附注之外，有两更旧的MD5证书：更新的认证(演示)应该是越新的SHA算法和有更长的有效期比更旧的证书示例)。：

```
Tue Jun 30 15:27:59 2015 Info: ICID 4420993 TLS failed: (336109761,
'error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
```

纠正措施

1.连接对Web (UI) ：**网络>证书**
2.验证您当前安排更旧的证书安装并且请有新的SHA证书示例。
3.基于更旧的证书示例适用的地方请用新的证书示例替换此。

典型地在以下部分可以发现这些证书适用：

- **网络>监听程序>然后监听程序>认证的名字**
- **邮件修正>目的地控制> Edit整体设置>认证**
- **网络> IP接口>选择与GUI访问> HTTPS认证产生关联的接口**
- **系统管理> LDAP > Edit设置>认证**

4. 一旦所有证书被替换了请从line命令验证TLS通信当前是成功的。

工作使用TLSv1.2协商的TLS通信示例：

```
Thu Jul  2 16:38:30 2015 Info: New SMTP ICID 4435675 interface Data1 (10.0.10.1)
address 209.85.213.182 reverse dns host mail-ig0-f182.google.com verified yes Thu Jul 2 16:38:30
2015 Info: ICID 4435675 ACCEPT SG UNKNOWNLIST match sbrs[0.0:10.0] SBRS 4.8 Thu Jul 2 16:38:30
2015 Info: ICID 4435675 TLS success protocol TLSv1.2 cipher AES128-GCM-SHA256
```

CLI纠正措施(如果GUI不可能被获取)

认证在有为HTTPS服务启用的一个认证的每个IP接口可能需要被修改。 为了修改认证在使用中为接口，请运行以下on命令CLI ：

1. 键入interfaceconfig。
2. select**编辑**。
3. 输入您希望编辑接口的编号。
4. 请使用返回键接受被提交的每个问题的当前设置。 当展示时适用的认证的选项，请选择证书示例：
   1.
   ```
   1. Ironport Demo Certificate
   2. Demo
   Please choose the certificate to apply:
   [1]> 2

   You may use "Demo", but this will not be secure.
   Do you really wish to use the "Demo" certificate? [N]> Y
   ```
5. 请完成跨步通过设置提示，直到所有配置问题完成。
6. 请使用返回键退出到主要CLI提示。
7. 保存您的对配置的更改的Usecommit。

   Note: 请切记在更改认证以后**确认**更改在使用中在接口。

Related Information

- TLS全面的设置指南在ESA
- Cisco电子邮件安全工具-终端用户指南
- Cisco安全管理工具-终端用户指南
- Technical Support & Documentation - Cisco Systems