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

目录

简介

本文描述为电子邮件安全版本9.5或以上将应用的，如果遇到与TLS通信的一个问题或者访问Web接口，在升级以后对AsyncOS必要的步骤在Cisco电子邮件安全工具(ESA)。

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**:下列是在设备应用的当前证书示例的一列出的应急方案。然而，下面的步骤可能设备也应用到所有MD5签名证书。

在执行升级对电子邮件安全版本9.5和以上的AsyncOS，在使用中其中任一个传统IronPort的证书示例，并且已应用为交付，接收或LDAP，可能经历错误，当尝试通过与一些域时的TLSv1/TLSv1.2通信。 TLS错误将引起所有入站或呼出会话发生故障。

如果证书应用对HTTPS接口，现代Web浏览器不能访问设备的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')
```

此错误是由应用的签名算法造成的是更旧的证书MD5;然而，用连接的设备/浏览器关联的证书只支持SHA签名基于算法。虽然，有的更旧的证书示例MD5签名是在设备同一时间新的SHA基于证书示例上述错误只将表明自己，如果MD5签名基于证书应用对指定的部分(即接收，交付等等)

下面从除新的证书示例(注意:之外，有两更旧的MD5证书设备的cli拉的示例更新的证书(演示)应该是越新的SHA算法和有一个更加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.导航对Web (UI) ：**网络>证书**
2.验证您当前安排更旧的证书安装并且有新的SHA证书示例。
3.基于更旧的证书示例应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应用：

- **网络>监听程序>然后监听程序>证书的名称**
- **邮件修正>目的地控制> Edit全局设置>证书**
- **网络> IP接口>选择接口关联与GUI访问> HTTPS证书**
- **系统管理> LDAP > Edit设置>证书**

4. 一旦所有证书替换请从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不可能访问)

有为HTTPS服务启用的一证书的证书在每个IP接口可能需要被修改。 为了修改证书在使用中为接口，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。 当能应用提交时证书的选项，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符，直到所有配置问题完成。
6. 请使用返回键退出到主CLI提示符。
7. 保存您的对配置的更改的Usecommit。

Note: 请切记在更改证书以后**确认**更改在使用中在接口。

相关信息

- TLS的全面的设置指南在ESA
- 思科电子邮件安全工具-最终用户指南
- Cisco安全管理设备-最终用户指南
- 技术支持和文档 - Cisco Systems