防止空或匿名密码器的协商在ESA和SMA

文档ID117864

已更新：二月19， 2015

贡献用Jai鳃和罗伯特Sherwin， Cisco TAC工程师。

相关产品

- 思科电子邮件安全工具

目录

简介

本文描述如何修改思科电子邮件安全工具(ESA)和Cisco安全管理设备(SMA)密码器设置为了防止空或匿名密码器的协商。本文适用于硬件基于和虚拟基于设备。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科ESA
- 思科SMA

使用的组件

本文档中的信息根据思科ESA和思科SMA的所有版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

防止空或匿名密码器的协商

此部分描述如何防止空或匿名密码器的协商在Cisco ESA运行电子邮件安全版本9.1和以上的AsyncOS，并且在Cisco SMA。

运行电子邮件安全版本9.1或以上的AsyncOS的ESAs

您能修改在ESA使用用**sslconfig**命令的密码器。为了防止空或匿名密码器的ESA协商，请输入**sslconfig**命令到ESA CLI并且应用这些设置：

- 入站简单邮件传输协议(SMTP)方法：**sslv3tlsv1**
- 入站SMTP密码器：**MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH**
- 出站SMTP方法：**sslv3tlsv1**
- 出站SMTP密码器：**MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH**

这是入站密码器的一配置示例：

```
CLI: > sslconfig

sslconfig settings:
  GUI HTTPS method:  sslv3tlsv1
  GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
  Inbound SMTP method:  sslv3tlsv1
  Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
  Outbound SMTP method:  sslv3tlsv1
  Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit inbound SMTP ssl settings.
- OUTBOUND - Edit outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
```

```
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]> 3

Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH
```

注意：设置GUI，入站和出站当必要时为每密码器。

自电子邮件安全版本8.5的AsyncOS， **sslconfig**命令通过GUI也是可用的。为了到达从GUI的这些设置，请导航对**系统管理> SSL配置> Edit设置**：

提示：巩固插槽紫菜(SSL)版本3.0 (RFC-6101)是过时和不安全协议。有在叫作*填充在Downgraded传统加密(长卷毛狗)攻击的Oracle* CVE-2014-3566的一个漏洞的SSLv3，由Cisco Bug ID CSCur27131跟踪。思科建议您禁用SSLv3，当您更换密码器，只使用传输层安全(TLS)时，并且选择*选项3* (TLS v1)。参考的Cisco Bug ID CSCur27131关于完整详细信息。

运行电子邮件安全版本9.5或以上的AsyncOS的ESAs

使用AsyncOS的介绍电子邮件安全版本9.5的，当前支持TLS v1.2。在前面部分仍然描述的命令运作;然而，您为在输出中v1.2将看到更新包括的TLS。

这是从CLI的一示例输出：

```
> sslconfig

sslconfig settings:
GUI HTTPS method: tlsv1/tlsv1.2
GUI HTTPS ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Inbound SMTP method: tlsv1/tlsv1.2
Inbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH
Outbound SMTP method: tlsv1/tlsv1.2
Outbound SMTP ciphers:
MEDIUM
HIGH
-SSLv2
-aNULL
@STRENGTH

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> inbound

Enter the inbound SMTP ssl method you want to use.
```

```
1. SSL v2
2. SSL v3
3. TLS v1/TLS v1.2
4. SSL v2 and v3
5. SSL v3 and TLS v1/TLS v1.2
6. SSL v2, v3 and TLS v1/TLS v1.2
[3]>
```

为了到达从GUI的这些设置，请导航对**系统管理> SSL Configuration>编辑设置…** ：

> **提示**：完整信息，参考版本9.5或以上的适当的ESA最终用户指南。

SMA

sslconfig命令为思科SMA不是可用的。

> **注意**： 此时，支持仅TLS v1; ESA只支持TLS v1.2。

您必须完成从SMA CLI的这些步骤为了修改SSL密码器：

1. 保存SMA配置文件到您的本地计算机。
2. 打开XML文件。
3. 搜索在XML的*<ssl>*部分：
```
<ssl>
   <ssl_inbound_method>sslv3tlsv1</ssl_inbound_method>
   <ssl_inbound_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_inbound_ciphers>
   <ssl_outbound_method>sslv3tlsv1</ssl_outbound_method>
   <ssl_outbound_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_outbound_ciphers>
   <ssl_gui_method>sslv3tlsv1</ssl_gui_method>
   <ssl_gui_ciphers>RC4-SHA:RC4-MD5:ALL</ssl_gui_ciphers>
 </ssl>
```
4. 修改如期望的一样密码器并且保存XML ：
```
<ssl>
<ssl_inbound_method>tlsv1</ssl_inbound_method>
<ssl_inbound_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_inbound_ciphers>
<ssl_outbound_method>tlsv1</ssl_outbound_method>
<ssl_outbound_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_outbound_ciphers>
<ssl_gui_method>tlsv1</ssl_gui_method>
<ssl_gui_ciphers>MEDIUM:HIGH:-SSLv2:-aNULL:@STRENGTH</ssl_gui_ciphers>
</ssl>
```
5. 装载在SMA上的新配置文件。
6. **提交**并且**确认**所有更改。

相关的思科支持社区讨论

思科支持社区是提出和解答问题、分享建议以及与同行协作的论坛。

有关本文档中所用的规则信息，请参阅 Cisco Technical Tips Conventions 。

已更新：二月19， 2015
文档ID117864