升级后，排除与SEG AsyncOS 15.0的旧Exchange Server连接故障

目录

[简介](#)

[使用的组件](#)

[问题](#)

[解决方案](#)

[相关信息](#)

简介

本文档介绍在升级到版本15.0后修复Exchange 2013（或更早版本）与SEG的连接问题的步骤。

使用的组件

- Exchange 2013或更早版本
- 思科安全电子邮件网关(SEG)版本15.0

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

问题

将SEG升级到版本15.0后，未在2013年以前的Exchange服务器之间建立连接。如果从CLI检查tophosts，可以看到域被标记为down(*):

```
mail.example.com > tophosts

Sort results by:

1. Active Recipients
2. Connections Out
3. Delivered Recipients
4. Hard Bounced Recipients
5. Soft Bounced Events
[1]> 1
```

```
Status as of:                   Sun Sep 03 11:44:11 2023 -03
Hosts marked with '*' were down as of the last delivery attempt.

                          Active  Conn.     Deliv.       Soft       Hard
#   Recipient Host        Recip.    Out     Recip.    Bounced    Bounced
1*  example.com          118      0          0          0     507
2*  alt.example.com      94       0        226          0     64
3*  prod.example.com     89       0          0          0     546
```

在邮件日志中，您可以看到由于出现“网络错误”原因导致到域的连接失败。

```
Thu Aug 29 08:16:21 2023 Info: Connection Error: DCID 4664840 domain: example.com IP: 192.0.2.10 port:
```

在数据包捕获中，您可以看到Exchange服务器在TLS协商后立即关闭与FIN数据包的连接。

解决方案

确认Exchange服务器是否在2013版或更早版本上，然后可以使用此密码字符串作为解决方法，以允许SEG连接到那些较旧的服务器。这样，在exchange升级到当前支持的版本之前，邮件可以传递。

```
ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL:!eNULL:!DES:!3DE
```

您可以通过命令行界面(CLI)或Web图形用户界面(GUI)输入此信息。
在CLI中：

```
mail.example.com> sslconfig

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.
- OTHER_CLIENT_TLSV10 - Edit TLS v1.0 for other client services.
- PEER_CERT_FQDN - Validate peer certificate FQDN compliance for Alert Over TLS, Outbound SMTP, updater
- PEER_CERT_X509 - Validate peer certificate X509 compliance for Alert Over TLS, Outbound SMTP, updater
[]> outbound

Enter the outbound SMTP ssl method you want to use.
1. TLS v1.1
2. TLS v1.2
3. TLS v1.0
[2]>

Enter the outbound SMTP ssl cipher you want to use.
[!aNULL:!eNULL]> ECDH+aRSA:ECDH+ECDSA:DHE+DSS+AES:AES128:AES256:!SRP:!AESGCM+DH+aRSA:!AESGCM+RSA:!aNULL
```

```
.....
Hit enter until you are back to the default command line.


mail.example.com> commit
```

在GUI中：
步骤1.选择System Administration(系统管理)选项卡。
步骤2.选择SSL Configuration。
步骤3.选择Edit Settings按钮。
步骤4.将Outbound SMTP SSL Cipher(s)更改为使用本文中提供的字符串。
步骤5.提交并提交更改。

相关信息

- AsyncOS 15.0用户指南：系统管理
- 更改ESA上与SSL/TLS配合使用的方法和密码
- 思科漏洞ID CSCwh48138 - ESA 15.0通过Exchange 2013的TLS进行电子邮件传送失败

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。