9.5 e AsyncOS mais novo para a upgrade de segurança do email com uma comunicação mais velha TLSv1.2 dos Certificados (MD5) a falhar

Índice

Introdução
Os Certificados do legado (MD5) fazem com que uma comunicação TLSv1.2 falhe em 9.5 AsyncOS para upgrades de segurança do email e mais novo
Ações Corretivas
Ações corretiva CLI (se o GUI não pode ser alcançado)
Informações Relacionadas
Cisco relacionado apoia discussões da comunidade

Introdução

Este documento descreve as etapas necessárias a ser aplicadas se encontrando uma edição com uma comunicação TLS, ou alcançando a interface da WEB, após o melhoramento a AsyncOS para a versão 9.5 mais recente da Segurança do email nas ferramentas de segurança do email de Cisco (ESA).

Os Certificados do legado (MD5) fazem com que uma comunicação TLSv1.2 falhe em 9.5 AsyncOS para upgrades de segurança do email e mais novo

> **Note**: O seguinte é uma ação alternativa listada para os Certificados atuais do programa demonstrativo aplicados no dispositivo. Contudo, as etapas abaixo podem igualmente dispositivo aplicar-se a todos os certificados assinados MD5.

Em cima de executar uma elevação a AsyncOS para a versão 9.5 mais recente da Segurança do email, alguns dos Certificados do programa demonstrativo de IronPort do legado ainda no uso e aplicados para a entrega, recepção ou LDAP, podem experimentar erros ao tentar comunicar-se através de TLSv1/TLSv1.2 com alguns domínios. O erro TLS fará com que todo o de entrada ou sessões externas falhem.

Se os Certificados são aplicados à relação HTTPS, os navegadores da Web modernos não alcançarão a interface da WEB do dispositivo.

Os logs do correio devem olhar similares ao exemplo seguinte:

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

Este erro é causado pelo algoritmo da assinatura aplicado ao certificado mais velho que é MD5;

contudo, os Certificados associados com o dispositivo/navegador de conexão apoiam somente algoritmos baseados assinatura SHA. Embora, os Certificados mais velhos do programa demonstrativo que tem a assinatura MD5 sejam no dispositivo o mesmo tempo o certificado baseado SHA novo do programa demonstrativo o erro acima manifestar-se-á somente se o certificado MD5 baseado assinatura é aplicado às seções especificadas (isto é recepção, entrega, etc.)

Está abaixo um exemplo puxado do CLI de um dispositivo que tenha ambos os Certificados MD5 mais velhos além do que o certificado novo do programa demonstrativo (nota: o certificado mais novo (programa demonstrativo) deve ser mais novo o algoritmo SHA e ter uma data de expiração mais longa do que os Certificados mais velhos do programa demonstrativo).:

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

Ações Corretivas

1. Navegue à Web (UI): **Rede > Certificados**
2. Verifique que você têm atualmente os Certificados mais velhos instalados e igualmente tenha o certificado novo do programa demonstrativo SHA.
3. Baseado em onde os Certificados mais velhos do programa demonstrativo são aplicados substitua isto com o certificado novo do programa demonstrativo.

Tipicamente estes Certificados podem ser encontrados ser aplicada nas seguintes seções:

- **Rede > ouvintes > então nome do ouvinte > do certificado**
- **O correio policia > controles do destino > edita configurações globais > certificado**
- **A rede > a interface IP > escolhem a relação associada com o acesso de GUI > o certificado HTTPS**
- **A administração do sistema > o LDAP > editam ajustes > certificado**

4. Uma vez que todos os Certificados foram substituídos verifique da linha de comando que uma comunicação TLS é agora bem sucedida.

Exemplo de trabalhar uma comunicação TLS que está sendo negociada usando TLSv1.2:

```
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
```

Ações corretiva CLI (se o GUI não pode ser alcançado)

O certificado pode precisar de ser alterado em cada interface IP que tem um certificado permitido para o serviço HTTPS. A fim alterar o certificado no uso para relações, execute por favor os comandos seguintes no CLI:

1. Datilografe o **interfaceconfig**.
2. Select **edita**.
3. Incorpore o número da relação que você deseja editar.
4. Use a chave do retorno para aceitar as configurações atual para cada pergunta apresentada. Quando a opção para que o certificado se aplique é apresentada, selecione o certificado do programa demonstrativo:

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. Termine pisar com as alertas dos ajustes até que todas as perguntas de configuração estejam terminadas.
6. Use a chave do retorno para retirar à alerta principal CLI.
7. Usecommit para salvar suas mudanças à configuração.

Note: Recorde por favor **comprometer** mudanças após ter mudado o certificado no uso na relação.

Informações Relacionadas

- Guia detalhado da instalação para o TLS no ESA
- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Dispositivo do Gerenciamento do Cisco Security - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems