Hoe de integratie van SMA en ESA aan te pakken als gevolg van een storing in het algoritme van de sleuteluitwisseling/algoritme.

Inhoud

Inleiding

Dit document beschrijft hoe de integratiefouten van Security Management-applicatie (SMA) en E-mail security applicatie (ESA) moeten worden aangepakt, wat resulteert in fouten: "*(3, 'kon geen matchend algoritme voor belangrijke uitwisseling vinden') of "Onverwacht EOF op verbinding*" en bijkomende symptomen.

Achtergrondinformatie

SMA-verbinding met het ESA bij de eerste integratie biedt SMA de volgende omwisselingsalgoritmen/sleutelalgoritmen aan het ESA:

```
kex_algorithms string: diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-
sha1,diffie-hellman-group14-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
encryption_algorithms_client_to_server string: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-
cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client string: aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-
cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

Nadat de SMA- en ESA-verbinding tot stand is gebracht, biedt het SMA de volgende omwisselingsalgoritmen/sleutelelementen aan het ESA:

```
kex_algorithms string: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-
sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-
hellman-group14-sha1,diffie-hellman-group1-sha1
encryption_algorithms_client_to_server string [truncated]: aes128-ctr,aes192-ctr,aes256-
ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-
poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-
cbc,arcfour,rijndael-cbc@lysator.liu.se
encryption_algorithms_server_to_client string [truncated]: aes128-ctr,aes192-ctr,aes256-
ctr,arcfour256,arcfour128,aes128-gcm@openssh.com,aes256-gcm@openssh.com,chacha20-
poly1305@openssh.com,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-
cbc,arcfour,rijndael-cbc@lysator.liu.se
```

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Probleem

Dit probleem bestaat bij het integreren van de SMA in het ESR vanuit de **GUI > Management-applicatie > Gecentraliseerde services > security applicaties of de CLI > applicatie-configuratie**. De kwestie zal leiden tot een fout bij de connectie, dit komt doordat het ESA een aantal van de kex algoritmen/algoritmen mist.

```
1. (3, 'Could not find matching key exchange algorithm.')
2. Error — Unexpected EOF on connect.
```

Oplossing

Om dit op te lossen moet de configuratie van het ESRs-algoritme worden teruggekocht naar de standaardwaarden die worden verstrekt:

```
lab.esa.com> sshconfig


Choose the operation you want to perform:
- SSHD - Edit SSH server settings.
- USERKEY - Edit SSH User Key settings
- ACCESS CONTROL - Edit SSH whitelist/blacklist
[]> sshd

ssh server config settings:
Public Key Authentication Algorithms:
        rsa1
        ssh-dss
        ssh-rsa
Cipher Algorithms:
        aes128-ctr
        aes192-ctr
        aes256-ctr
        aes128-cbc
        3des-cbc
        blowfish-cbc
        cast128-cbc
        aes192-cbc
        aes256-cbc
        rijndael-cbc@lysator.liu.se
MAC Methods:
        hmac-md5
        hmac-sha1
        umac-64@openssh.com
        hmac-ripemd160
        hmac-ripemd160@openssh.com
        hmac-sha1-96
        hmac-md5-96
Minimum Server Key Size:
        1024
KEX Algorithms:
        diffie-hellman-group-exchange-sha256
        diffie-hellman-group-exchange-sha1
        diffie-hellman-group14-sha1
        diffie-hellman-group1-sha1
        ecdh-sha2-nistp256
        ecdh-sha2-nistp384
        ecdh-sha2-nistp521
```

De output van **CLI > ssheconfig > sshd** op de stapsgewijze instelling:

```
[]> setup

Enter the Public Key Authentication Algorithms do you want to use
[rsa1,ssh-dss,ssh-rsa]>

Enter the Cipher Algorithms do you want to use
[aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-
cbc,aes256-cbc,rijndael-cbc@lysator.liu.se]>

Enter the MAC Methods do you want to use
[hmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-
96,hmac-md5-96]>

Enter the Minimum Server Key Size do you want to use
[1024]>

Enter the KEX Algorithms do you want to use
[diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha1,diffie-hellman-group1-sha1,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521]>
```

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie – Cisco Systems
- Best Practices for Centralised Policy Virus en Outbreak Quarantine
- Uitgebreide handleiding voor ESA Spam Quarantine setup met SMA