

Begrijp de Algoritmen van SSH Crypto op ISE

3.3 Patch 4

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereiste componenten](#)

[Doelstellingen](#)

[Functionele voordelen](#)

[Belangrijkste kenmerken geïmplementeerd](#)

[CLI-opdrachten](#)

[Configureerbaar SSH-hostsleutelalgoritme](#)

[Configureerbaar SSHD HostKey Algoritme](#)

[Probleemoplossing](#)

[Verifiëren](#)

[Logfragment:](#)

[FAQ](#)

Inleiding

Dit document beschrijft over SSH Crypto Algoritmen op ISE-versie 3.3 Patch 4

Voorwaarden

U moet de basiskennis van Cisco Identity Service Engine (ISE) hebben

Kennis over SSH-protocol

Kennis over host-key algoritmen

Vereiste componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies

- Patch 4 voor Cisco Identity Services Engine 3.3

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 live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Doelstellingen

Ontwikkel en implementeer CLI-opdrachten om configureerbare SSH-algoritmen te ondersteunen, waarbij beveiligingskwetsbaarheden worden aangepakt volgens uw vereisten.

Functionele voordelen

1. NIST-richtlijnen voor uitgebreide SSH-beveiliging.
2. Flexibele configuratieopties voor SSH-algoritmen om aan specifiek beveiligingsbeleid te voldoen.

Belangrijkste kenmerken geïmplementeerd

1. Configureerbaar HostKey en Hostkey Algoritme van CLI.
2. Ondersteuning voor ecdsa-sha2-nistp256 en ed host key.
3. Ondersteuning voor hmac-sha2-256 en hmac-sha2-512 voor beveiligde SSH-verbindingen

CLI-opdrachten

- Service sh-host-key-algoritme
- Service- en hostsleutel
- Service-shd host-key-algoritme
- Netwerkalgoritme voor servicesmodule

Configureerbaar SSH-hostsleutelalgoritme

Het SSH HostKey Algoritme voor externe servercommunicatie configureren

Opdracht: `asc-ise33p4/admin (config)# service-sh host-key-algoritme?`

Mogelijke aanvullingen:

`ecdsa-sha2-nistp256` Configureren `ecdsa-sha2-nistp256` algo

`rsa-sha2-256` `Rsa-sha2-256` algo configureren

`rsa-sha2-512` `Rsa-sha2-512` instellen

`sh-rsa-algo` configureren



Opmerking: Dit is voor SSH

Configureerbaar SSHD HostKey Algoritme

Om de SSHD HostKey voor SSH-serververificatie te configureren.

Opdracht: `asc-ise33p4/admin (config)# Service sshd host-key?`

Mogelijke aanvullingen:

`host-ecdsa-256` De SSH-host-ecdsa 256-toets configureren

`host-ed25519` De SSH host-ed25519-toets configureren

`host-rsa` Configureren ssh host rsa-toets

Om het SSHD Host Key Algorithm voor SSH-serververificatie te configureren.

Opdracht: asc-ise33p4/admin(config)#service sshd host-key-algoritme ?

Mogelijke aanvullingen:

ecdsa-sha2-nistp256 Configureren ecdsa-sha2-nistp256 algo

rsa-sha2-256 Rsa-sha2-256 algo configureren

rsa-sha2-512 Rsa-sha2-512 instellen

sh-ed25519 Ssh-ed configureren25519 algo

Om SSHD MAC-algoritme te configureren voor SSH-serververificatie.

Opdracht: asc-ise33p4/admin(config)#service sshd mac-algoritme ?

Mogelijke aanvullingen:

hmac-sha1 Hmac-sha1-algoritme configureren

hmac-sha1-etm-openssh.com Configureren hmac-sha1-etm-openssh.com algo

hmac-sha2-256 Configureren hmac-sha2-256 algo

hmac-sha2-256-etm-openssh.com Configureren hmac-sha2-256-etm@openssh.com

hmac-sha2-512 Configureren hmac-sha2-512 algoritme

hmac-sha2-512-etm-openssh.com Configureren hmac-sha2-512-etm@openssh.com



Opmerking: Dit is voor SSHD

Probleemoplossing

Verifiëren

SSH:

```
isepri33/admin(config)#service ssh host-key-algoritme ecdsa-sha2-nistp256
```

```
isepri33/admin#show-service voor in bedrijf zijnde configuratiebestanden  
service sh host-key-algoritme ecdsa-sha2-nistp256
```

SSHD:

```
isepri33/admin(config)#service sshd host-key-algoritme ecdsa-sha2-nistp256
```

isepri33/admin#show-serviceskaart voor in bedrijf zijnde configuratie
servicesmodule inschakelen
Service Grid-encryptie-algoritme aes128-ctr aes128-gcm-openssh.com aes256-ctr aes256-gcm-openssh.com chacha20-poly1305-openssh.com
service-shd host-key-algoritme ecdsa-sha2-nistp256
service sshd mac-algoritme hmac-sha1 hmac-sha2-256 hmac-sha2-512
service-shelf host-key host-rsa

Logfragment:

isepri33/admin#show-logboekstelsysteem confd/confd.log
2025-03-18 08:35:25,241 [INFO] service_conf.py update_host_key_algorithms regel:575
Bijgewerkte SSH Host Keys Algoritmen met succes
2025-03-18 08:35:39,056 [INFO] service_conf.py update_host_key_algorithms regel:567 Host
sleutel Algoritmen: ecdsa-sha2-nistp256
2025-03-18 08:35:39,260 [INFO] service_conf.py start_sshd lijn:259 Gerestaureerde sshd met
succes

2025-03-18 08:48:20,194 [INFO] service_conf.py update_host_key_algorithms regel:567 Host
sleutel Algoritmen: ecdsa-sha2-nistp256
2025-03-18 08:48:20,396 [INFO] service_conf.py start_sshd lijn:259 Gerestaureerd sshd met
succes
2025-03-18 08:48:20,400 [INFO] service_conf.py update_host_key_algorithms regel:575
Bijgewerkte SSH Host Keys Algoritmen met succes
2025-03-18 08:49:00,442 [INFO] service_conf.py update_host_key_algorithms regel:567 Host
sleutel Algoritmen: ecdsa-sha2-nistp256
2025-03-18 08:49:00,672 [INFO] service_conf.py start_sshd lijn:259 Gerestaureerd sshd met
succes
2025-03-18 08:49:00,674 [INFO] service_conf.py update_host_key_algorithms regel:575
Bijgewerkte SSH Host Keys Algoritmen met succes

FAQ

Vraag: Wat is het standaard SSH host-sleutelalgoritme ingeschakeld op ISE?

Antwoord: Dit zijn:

- rsa-sha2-256
- rsa-sha2-512

Vraag: Wat is het standaard SSHD MAC Key Algoritme?

Antwoord: Dit zijn:

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512

Vraag: Wat is de standaard SSHD host-key?

Antwoord: host-rsa

Vraag: Wat zijn de standaard SSH host-sleutel?

Antwoord: Dit zijn:

- rsa-sha2-256
- rsa-sha2-512
- ssh-rsa

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.