Comprensión de los algoritmos criptográficos SSH en el parche 4 de ISE 3.3

Contenido

Introducción

Este documento describe los algoritmos criptográficos SSH en ISE versión 3.3 Parche 4

Requisitos previos

Debe contar con los conocimientos básicos de Cisco Identity Service Engine (ISE)

Conocimiento sobre el protocolo SSH

Conocimiento de los algoritmos de clave de host

Componentes necesarios

La información que contiene este documento se basa en estas versiones de software y hardware

- Parche 4 de Cisco Identity Services Engine 3.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Objetivos

Desarrolle e implemente comandos CLI para admitir algoritmos SSH configurables y hacer frente a las vulnerabilidades de seguridad según sus requisitos.

Ventajas funcionales

1. Cumplimiento mejorado de la seguridad SSH con las directrices NIST.
2. Opciones de configuración flexibles para que los algoritmos SSH cumplan con las políticas de seguridad específicas.

Funciones clave implementadas

1. Algoritmo de clave de host y clave de host configurable desde CLI.
2. Compatibilidad con ecdsa-sha2-nistp256 y la clave de host ed.
3. Compatibilidad con hmac-sha2-256 y hmac-sha2-512 para conexiones SSH seguras

Comandos CLI

- Service ssh host-key-algorithm
- Service sshd host-key
- Service sshd host-key-algorithm
- Service sshd mac-algorithm

Algoritmo de clave de host SSH configurable

Para Configurar el Algoritmo SSH HostKey para la Comunicación Externa del Servidor

Comando: asc-ise33p4/admin(config)# service ssh host-key-algorithm ?

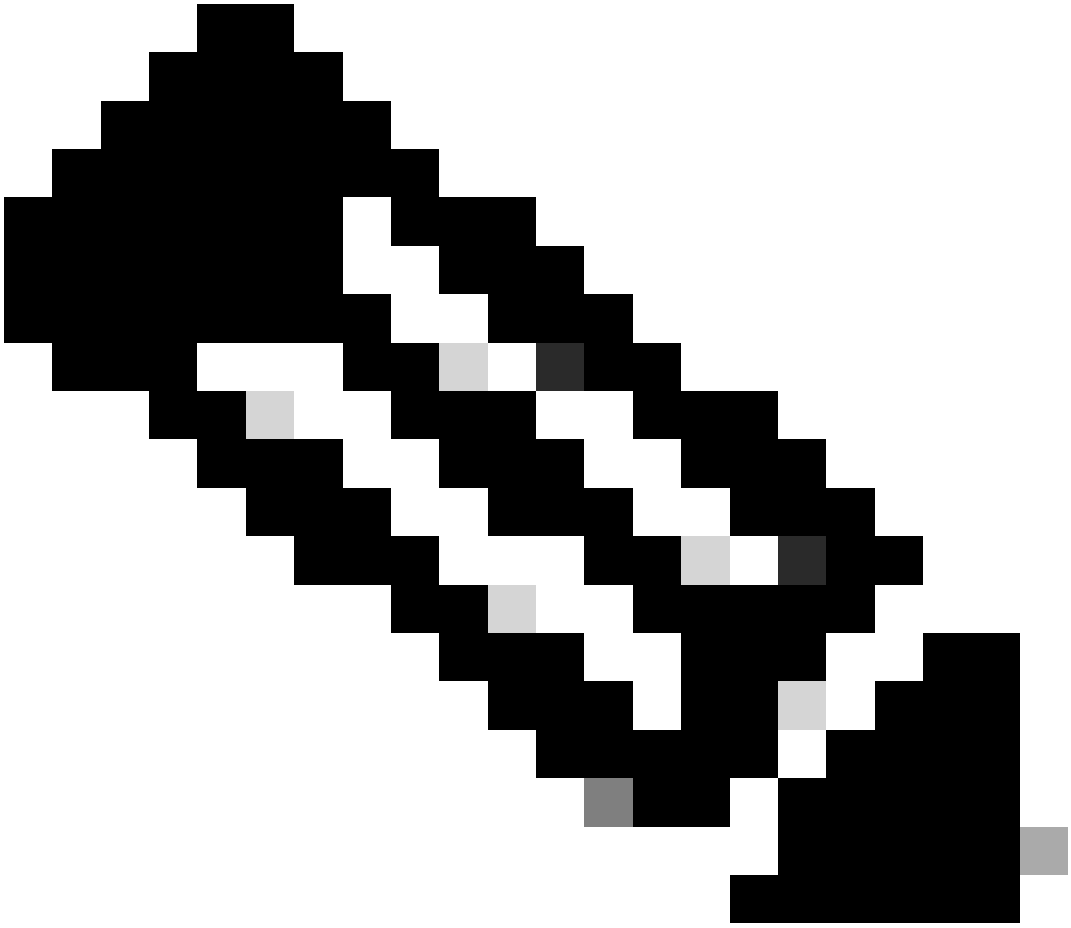
Posibles finalizaciones:

ecdsa-sha2-nistp256 Configuración de ecdsa-sha2-nistp256 algo

rsa-sha2-256 Configurar rsa-sha2-256 algo

rsa-sha2-512 Configure rsa-sha2-512 algo

ssh-rsa Configure ssh-rsa algo



Nota: Esto es para SSH

Algoritmo HostKey SSHD configurable

Para configurar la clave de host SSHD para la autenticación del servidor SSH.

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

Posibles finalizaciones:

host-ecdsa-256 Configure ssh host ecdsa 256 key

host-ed25519 Configurar ssh host ed25519 key

host-rsa Configure ssh host rsa key

Para Configurar el Algoritmo de Clave de Host SSHD para la Autenticación del Servidor SSH.

Comando: asc-ise33p4/admin(config)#service sshd host-key-algorithm ?

Posibles finalizaciones:

ecdsa-sha2-nistp256 Configuración de ecdsa-sha2-nistp256 algo

rsa-sha2-256 Configurar rsa-sha2-256 algo

rsa-sha2-512 Configure rsa-sha2-512 algo

ssh-ed25519 Configurar ssh-ed25519 algo

Para configurar el algoritmo SSHD MAC para la autenticación del servidor SSH.

Comando: asc-ise33p4/admin(config)#service sshd mac-algorithm ?

Posibles finalizaciones:

hmac-sha1 Configure hmac-sha1 algo

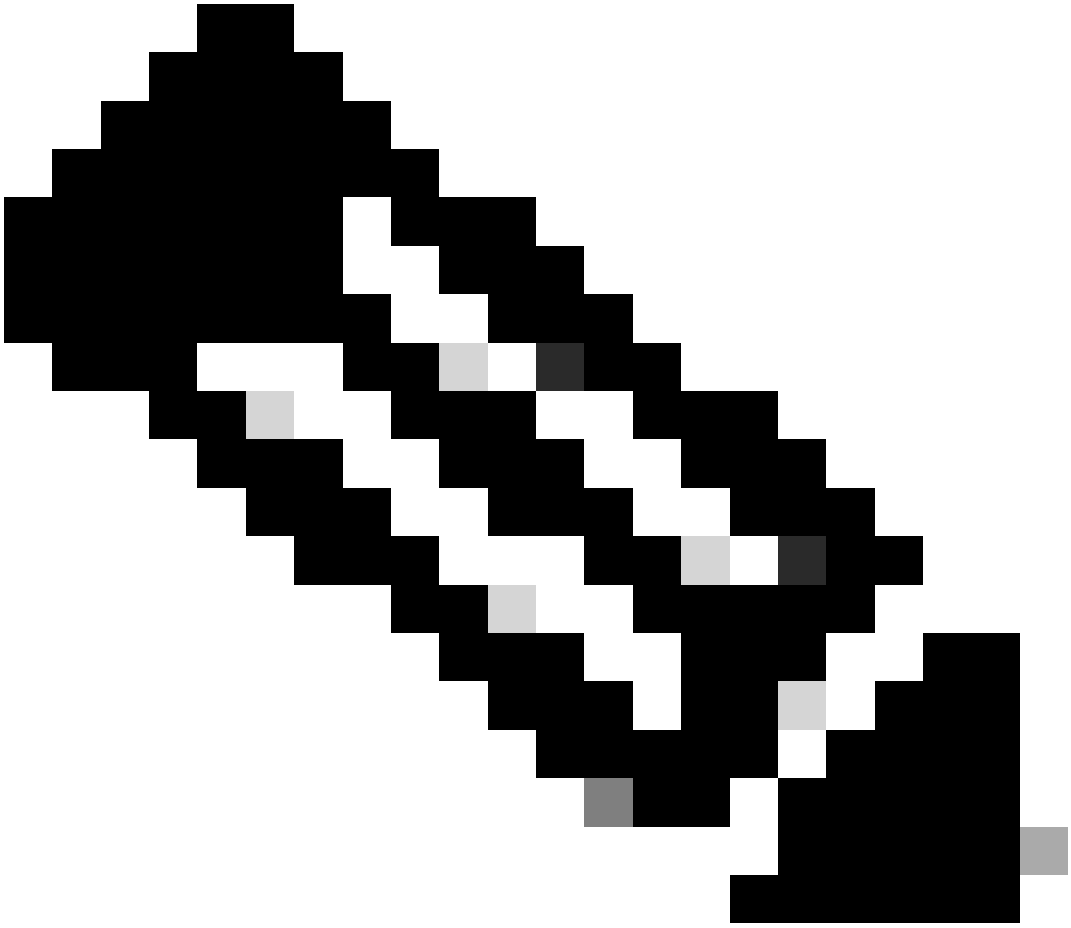
hmac-sha1-etm-openssh.com Configure hmac-sha1-etm-openssh.com algo

hmac-sha2-256 Configurar hmac-sha2-256 algo

hmac-sha2-256-etm-openssh.com Configure hmac-sha2-256-etm@openssh.com algo

hmac-sha2-512 Configurar hmac-sha2-512 algo

hmac-sha2-512-etm-openssh.com Configure hmac-sha2-512-etm@openssh.com algo



Nota: Esto es para SSHD

Resolución de problemas

Verificación

SSH:
isepri33/admin(config)#service ssh host-key-algorithm ecdsa-sha2-nistp256

isepri33/admin#show running-config service ssh
service ssh host-key-algorithm ecdsa-sha2-nistp256

SSHD:

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

```
isepri33/admin#show running-config service sshd
service sshd enable
service sshd encryption-algorithm aes128-ctr aes128-gcm-openssh.com aes256-ctr aes256-gcm-openssh.com chacha20-poly1305-openssh.com
service sshd host-key-algorithm ecdsa-sha2-nistp256
service sshd mac-algorithm hmac-sha1 hmac-sha2-256 hmac-sha2-512
service sshd host-key host-rsa
```

Fragmento de registro:

```
isepri33/admin#show logging system confd/confd.log
2025-03-18 08:35:25,241 [INFO] service_conf.py update_host_key_algoritms line:575 Algoritmos de claves de host SSH actualizados con éxito
2025-03-18 08:35:39,056 [INFO] service_conf.py update_host_key_algoritms line:567 Algoritmos de clave de host: ecdsa-sha2-nistp256
2025-03-18 08:35:39,260 [INFO] service_conf.py restart_sshd línea:259 Se reinició sshd con éxito

2025-03-18 08:48:20,194 [INFO] service_conf.py update_host_key_algoritms line:567 Algoritmos de clave de host: ecdsa-sha2-nistp256
2025-03-18 08:48:20,396 [INFO] service_conf.py restart_sshd línea:259 Se reinició sshd con éxito
2025-03-18 08:48:20,400 [INFO] service_conf.py update_host_key_algoritms line:575 Algoritmos de claves de host SSH actualizados con éxito
2025-03-18 08:49:00,442 [INFO] service_conf.py update_host_key_algoritms line:567 Algoritmos de clave de host: ecdsa-sha2-nistp256
2025-03-18 08:49:00,672 [INFO] service_conf.py restart_sshd line:259 Se reinició sshd con éxito
2025-03-18 08:49:00,674 [INFO] service_conf.py update_host_key_algoritms line:575 Algoritmos de claves de host SSH actualizados con éxito
```

Preguntas frecuentes

Pregunta: ¿Cuál es el algoritmo de clave de host SSH predeterminado habilitado en ISE?

Respuesta: Las fallas son las siguientes:

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

Pregunta: ¿Cuáles son los algoritmos de clave MAC SSHD predeterminados?

Respuesta: Las fallas son las siguientes:

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

Pregunta: ¿Cuál es la clave de host SSHD predeterminada?

Respuesta: host-rsa

Pregunta: ¿Cuáles son las claves de host SSH predeterminadas?

Respuesta: Las fallas son las siguientes:

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).