Comprendere gli algoritmi di crittografia SSH su ISE 3.3 Patch 4

Sommario

Introduzione

Questo documento descrive gli algoritmi di crittografia SSH su ISE versione 3.3, patch 4

Prerequisiti

È necessario avere le conoscenze base di Cisco Identity Service Engine (ISE)

Conoscenza del protocollo SSH

Conoscenze sugli algoritmi Host-Key

Componenti richiesti

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware

- Patch 4 per Cisco Identity Services Engine 3.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Obiettivi

Sviluppo e implementazione di comandi CLI per supportare algoritmi SSH configurabili, risolvendo le vulnerabilità della sicurezza in base ai requisiti aziendali.

Vantaggi funzionali

1. Conformità della sicurezza SSH migliorata con le linee guida NIST.
2. Opzioni di configurazione flessibili per gli algoritmi SSH in modo da soddisfare le policy di sicurezza specifiche.

Caratteristiche principali implementate

1. HostKey e Hostkey Algorithm configurabili dalla CLI.
2. Supporto per ecdsa-sha2-nistp256 e chiave host end.
3. Supporto per hmac-sha2-256 e hmac-sha2-512 per connessioni SSH protette

Comandi CLI

- Service ssh host-key-algorithm
- Service sshd host-key
- Service sshd host-key-algorithm
- Algoritmo mac SSHD del servizio

Algoritmo SSH HostKey configurabile

Configurazione dell'algoritmo SSH HostKey per la comunicazione con il server esterno

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

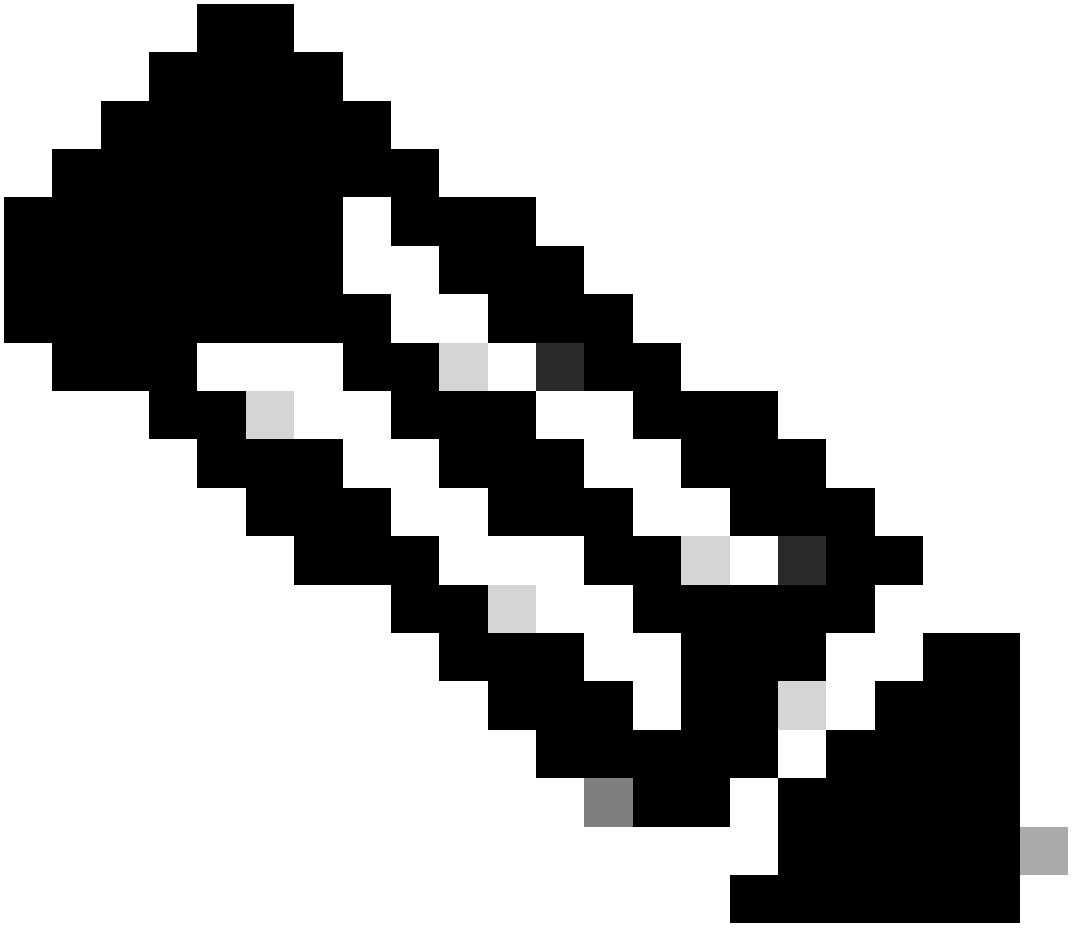
Completamenti possibili:

ecdsa-sha2-nistp256 Configurazione dell'algo ecdsa-sha2-nistp256

rsa-sha2-256 Configurazione dell'algo rsa-sha2-256

rsa-sha2-512 Configurare l'allarme rsa-sha2-512

ssh-rsa Configurazione del logo ssh-rsa



Nota: Questo è per SSH

Algoritmo SSHD HostKey configurabile

Per configurare la chiave host SSHD per l'autenticazione del server SSH.

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

Completamenti possibili:

host-ecdsa-256 Configurare l'host ssh chiave ecdsa 256

host-ed25519 Configurazione della chiave ssh host ed25519

host-rsa Configurare la chiave rsa dell'host ssh

Per configurare l'algoritmo SSHD Host Key per l'autenticazione del server SSH.

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

Completamenti possibili:

ecdsa-sha2-nistp256 Configurazione dell'algo ecdsa-sha2-nistp256

rsa-sha2-256 Configurazione dell'algo rsa-sha2-256

rsa-sha2-512 Configurare l'allarme rsa-sha2-512

ssh-ed2519 Configurazione dell'algo ssh-ed25519

Per configurare l'algoritmo MAC SSHD per l'autenticazione del server SSH.

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

Completamenti possibili:

hmac-sha1 Configurazione del logo hmac-sha1

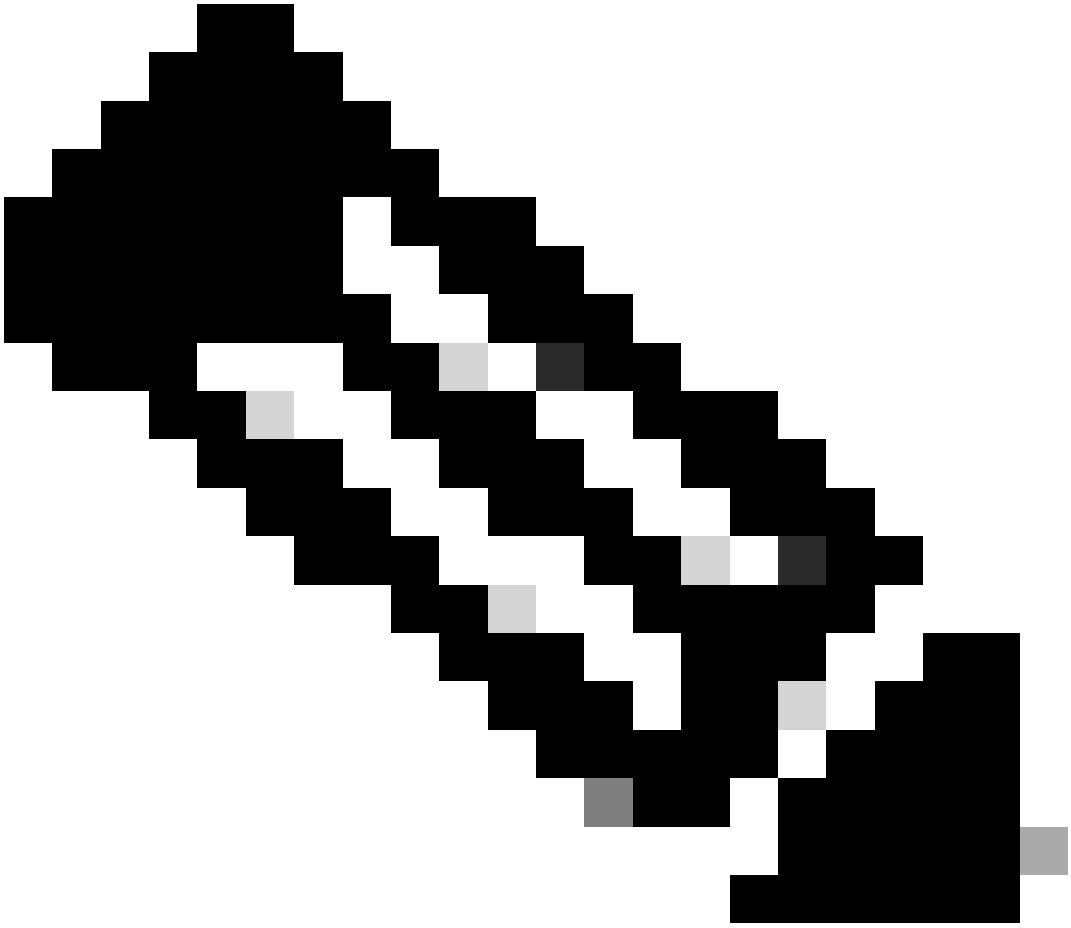
hmac-sha1-etm-openssh.com Configurare hmac-sha1-etm-openssh.com algo

hmac-sha2-256 Configurazione del logo hmac-sha2-256

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

hmac-sha2-512 Configurare l'hmac-sha2-512 algo

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



Nota: Per SSHD

Risoluzione dei problemi

Verifica

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

Frammento di log:

isepri33/admin#show logging system confd/confd.log
2025-03-18:35:25,241 [INFO] service_conf.py update_host_key_algorithms line:575
Aggiornamento degli algoritmi delle chiavi host SSH completato
2025-03-18 08:35:39,056 [INFO] service_conf.py update_host_key_algorithms linea:567 Algoritmi chiave host: ecdsa-sha2-nistp256
2025-03-18 08:35:39,260 [INFO] service_conf.py restart_sshd line:259 Riavvio riuscito di sshd

2025-03-18 08:48:20,194 [INFO] service_conf.py update_host_key_algorithms linea:567 Algoritmi chiave host: ecdsa-sha2-nistp256
2025-03-18 08:48:20,396 [INFO] service_conf.py restart_sshd line:259 Riavvio riuscito di sshd
2025-03-18:08:20,400 [INFO] service_conf.py update_host_key_algorithms line:575
Aggiornamento degli algoritmi delle chiavi host SSH completato
2025-03-18 08:49:00,442 [INFO] service_conf.py update_host_key_algorithms linea:567 Algoritmi chiave host: ecdsa-sha2-nistp256
2025-03-18 08:49:00,672 [INFO] service_conf.py restart_sshd line:259 Riavvio riuscito di sshd
2025-03-18 08:49:00,674 [INFO] service_conf.py update_host_key_algorithms line:575
Aggiornamento degli algoritmi delle chiavi host SSH completato

Domande frequenti

Domanda: Qual è l'algoritmo SSH Host Key predefinito abilitato su ISE?

Risposta. più di un'opzione:

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

Domanda: Qual è l'algoritmo predefinito per la chiave MAC SSHD?

Risposta. più di un'opzione:

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

Domanda: Qual è la chiave host SSHD predefinita?

Risposta. host-rsa

Domanda: Dove sono le chiavi host SSH predefinite?

Risposta. più di un'opzione:

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).