Come verificare che l'ESA accetti solo connessioni SSH da client che usano SSH v2?

Sommario

Introduzione

In questo documento viene descritto come rivedere e configurare le versioni di autenticazione SSH su Cisco Email Security Appliance (ESA).

Come verificare che l'ESA accetti solo connessioni SSH da client che usano SSH v2?

L'ESA può essere configurata per consentire le connessioni Secure Shell (SSH). Le connessioni SSH criptano il traffico tra l'host di connessione e l'ESA. In questo modo vengono protette informazioni di autenticazione quali nome utente e password. Il protocollo SSH è disponibile in due versioni principali: versione 1 (SSH v1) e versione 2 (SSH v2). Essendo più recente, SSH v2 è più sicuro di SSH v1, quindi molti amministratori ESA preferiscono consentire solo le connessioni dai client che usano SSH v2.

Nelle versioni di AsyncOS fino alla versione 7.6.3, la disabilitazione delle connessioni SSH v1 può essere effettuata dalla CLI con **sshconfig**:

```
mail3.example.com> sshconfig
Currently installed keys for admin:
Choose the operation you want to perform:
- NEW - Add a new key.
- USER - Switch to a different user to edit.
- SETUP - Configure general settings.
[]> setup
SSH v1 is currently ENABLED.
Choose the operation you want to perform:
- DISABLE - Disable SSH v1
[]> DISABLE
```

Nelle versioni AsyncOS 8.x e successive, l'opzione di disabilitazione di SSH v1 non esiste con **sshconfig**. Se SSH v1 è stato abilitato prima dell'aggiornamento della versione 8.x, SSH v1 rimarrà abilitato e accessibile sull'ESA anche dopo il completamento dell'aggiornamento, anche se tutto il supporto per SSH v1 è stato rimosso. Questo può essere un problema per gli amministratori che eseguono regolarmente controlli di sicurezza e test di penetrazione.

Poiché tutto il supporto per SSH v1 è stato rimosso, è necessario aprire una richiesta di supporto per disabilitare SSHv1.

Eseguire il seguente comando da un host Linux/Unix esterno o da un'altra connessione CLI applicabile di scelta, per verificare se SSH v1 è abilitato o disabilitato per l'ESA in questione:

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
Protocol major versions differ: 1 vs. 2
```

L'output previsto è "Le versioni principali del protocollo differiscono: 1 vs. 2", per segnalare che SSH v1 è disabilitato. In caso contrario, e SSH v1 è ancora abilitato, verrà visualizzato:

```
robert@my_ubuntu:~$ ssh -1 admin@192.168.0.199
Password:
Response:
Last login: Thu Oct 30 14:53:40 2014 from 192.168.0.3
Copyright (c) 2001-2013, Cisco Systems, Inc.

AsyncOS 8.0.1 for Cisco IronPort C360 build 023

Welcome to the Cisco IronPort C360 Messaging Gateway(tm) Appliance
myesa.local>
```

Questo output segnalerebbe che SSH v1 è ancora in uso e potrebbe causare insicurezza nell'ESA dopo l'aggiornamento a 8.x o versioni successive. Questo può essere portato all'attenzione con un test di penetrazione o un audit di sicurezza, e identificare un gap significativo. Per risolvere il problema, è necessario aprire una richiesta di assistenza e richiederne la correzione. Sarà necessario essere in grado di fornire un tunnel di supporto dall'ESA per il supporto tecnico Cisco.

Informazioni correlate

- CSCuo46017: SSHv1 rimane abilitato dopo l'aggiornamento e non può essere disabilitato
- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems