Reimpostazione password FTD firewall protetto Dopo perdita password

Problema

Firewall Threat Defense (FTD) è diventato inaccessibile tramite CLI a causa di una password di amministratore locale persa. Impossibile accedere al nodo interessato per scopi amministrativi. L'ipotesi iniziale era che la password dell'amministratore fosse stata modificata rispetto a quella predefinita e fosse sconosciuta, il che avrebbe comportato il rischio che fosse necessaria una reimpostazione completa (reimage) per ripristinare l'accesso e le credenziali predefinite. Sono sorte domande specifiche in merito alla corretta procedura per gestire questa situazione:

Ambiente

- Cisco Secure Firewall 1000, 2100 e 3100 FTD gestito da Firepower Management Center

Risoluzione

La risoluzione implicava il tentativo di accedere al dispositivo FTD interessato utilizzando le credenziali di amministratore predefinite prima di procedere con la procedura di ricreazione dell'immagine più complessa.

1: Prima di iniziare, tentare di accedere al dispositivo FTD interessato utilizzando le credenziali di amministratore predefinite di fabbrica.

```
Username: admin
Password: Admin123
```

Questa operazione deve essere eseguita per prima in quanto potrebbe eliminare la necessità di procedure di ripristino con interruzioni maggiori.

2: Se le credenziali predefinite sono escluse, reimpostare la password dell'amministratore su un nuovo valore noto tramite la procedura di modifica della password CLI FTD standard.

Processo di ricreazione immagine: Cisco Secure Firewall ASA e guida alla ricreazione di immagini per la difesa dalle minacce

- Eseguire la ricreazione completa dell'immagine del dispositivo FTD interessato, attenendosi alla procedura descritta nella documentazione di Cisco.
- Ripristinare le credenziali predefinite di fabbrica tramite il processo di ricreazione immagine.

Causa

La causa principale è stata che la password dell'amministratore sul dispositivo FTD interessato non è mai stata modificata rispetto all'impostazione predefinita di fabbrica durante la distribuzione iniziale. La perdita dell'accesso è dovuta al presupposto errato che la password fosse sconosciuta, piuttosto che a una effettiva perdita di credenziali. Il dispositivo è rimasto accessibile utilizzando le credenziali di amministratore predefinite per tutta la durata dell'incidente.

Contenuto correlato

- Sostituzione dell'unità difettosa in Secure Firewall Threat Defense of High Availability
- Guida alla risoluzione dei problemi di Cisco FXOS per la difesa dalle minacce del firewall: Gestione delle immagini
- Cisco Secure Firewall ASA e guida alla ricreazione di immagini per la difesa dalle minacce
- Configurazione, verifica e risoluzione dei problemi relativi alla registrazione delle periferiche Firepower
- Configurazione della funzionalità FTD High Availability nei dispositivi Firepower
- Supporto tecnico Cisco e download

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).