

Aggiornamento motore di snort bloccato durante l'aggiornamento FTD a causa del rilevamento dei criteri personalizzati

Sommario

Problema

Durante un aggiornamento FTD dalla versione 7.2 alla 7.4.4 su un HA FPR-4115 gestito da FMC, l'aggiornamento del motore Snort allo Snort 3 viene bloccato con messaggi di errore che indicano l'impossibilità di convertire le regole personalizzate Snort 2 o l'utilizzo di criteri di analisi di rete o intrusione personalizzati. Il messaggio di errore specifico indica: "Impossibile eseguire l'aggiornamento a Snort 3. Il dispositivo utilizza almeno un criterio di intrusione personalizzato o un criterio di analisi della rete." Un messaggio di errore più dettagliato fa riferimento all'impossibilità di convertire le regole personalizzate Snort 2 e rimanda a `/var/sf/htdocs/ips/snort.rej` per ulteriori informazioni. La preoccupazione è se questo errore impedirebbe la migrazione allo Snort 3 e la funzionalità di ispezione dell'impatto.

Ambiente

- Cisco Secure Firewall Firepower versione 7.3
- Firepower Management Center (FMC) versione 7.7.11
- Dispositivi FTD in configurazione ad alta disponibilità (HA, High Availability)
- Hardware: FPR-4115
- Percorso aggiornamento: da FTD 7.2 a 7.4.4
- Versione più recente di VDB prima dell'aggiornamento
- La sezione Regole locali in Oggetti > Regole intrusione > Ordina 2 Tutte le regole è vuota

Risoluzione

Il messaggio di errore che blocca l'aggiornamento del motore Snort è un comportamento documentato correlato all'ID bug Cisco CSCwn46794 e non rappresenta un blocco funzionale quando non esistono regole personalizzate Snort 2.

Fasi di verifica

Passaggio 1: Verificare lo stato delle regole personalizzate per gli snort 2

Passare all'interfaccia di FMC e verificare le regole personalizzate Snort 2:

Passaggio 2: Confermare la versione di VDB

Prima di procedere con l'aggiornamento, verificare che la versione del database di vulnerabilità (VDB) sia la più recente.

Passaggio 3: Rivedere i dettagli dell'errore

Controllare le informazioni dettagliate sull'errore nel file di riferimento:

```
/var/sf/htdocs/ips/snort.rej
```

Processo di aggiornamento

Quando si conferma che la sezione "Regole locali" è vuota (nessuna regola personalizzata Snort 2 presente), l'aggiornamento può continuare nonostante il messaggio di errore. L'errore di blocco è un falso positivo in questo scenario e non indica le regole personalizzate effettive che devono essere convertite.

Fase 1: procedere con l'aggiornamento Snort 3

Continuare con il processo di aggiornamento FTD alla versione 7.4.4, che include l'aggiornamento del motore Snort 3.

Passaggio 2: Convalida post-aggiornamento

Al termine dell'aggiornamento, verificare il flusso del traffico per confermare il comportamento previsto con il motore Snort 3.

Fase 3: Monitorare le prestazioni del sistema

Verificare che la funzionalità di ispezione funzioni come previsto con il nuovo motore Snort 3.

Causa

Il messaggio di blocco dell'aggiornamento è un comportamento documentato associato all'ID bug Cisco CSCwn46794. In seguito a questo bug, il sistema visualizza un messaggio di errore relativo ai criteri personalizzati per l'intrusione o ai criteri di analisi della rete anche se non esistono regole personalizzate specifiche che richiedono la conversione. Il messaggio di errore viene visualizzato come falso positivo quando la sezione Regole locali è vuota, ma la convalida precedente l'aggiornamento del sistema identifica in modo errato la presenza di criteri personalizzati.

Contenuto correlato

- [ID bug Cisco CSCwn46794](#)

- [ID bug Cisco CSCwk0719](#)
- [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).