Chiarire il processo di aggiornamento di VDB su FMC

Sommario

Problema

Quando gli aggiornamenti VDB (Vulnerability Database) vengono eseguiti in ritardo, gli amministratori devono capire se gli aggiornamenti VDB sono cumulativi e se possono ignorare le versioni intermedie.

In questo esempio, il problema si verifica quando si esegue l'aggiornamento da VDB versione 393 alla versione 427. In particolare, non è chiaro se sono necessari più passaggi di aggiornamento o se è supportato un percorso di aggiornamento diretto. Inoltre, emergono problemi relativi alle potenziali interruzioni del servizio durante l'aggiornamento del VDB e il successivo processo di distribuzione delle regole.

Ambiente

- Software Secure Firewall Management Center (FMC) versione 7.4.2.4. Sono interessate anche altre versioni software.
- Firewall Threat Defense (FTD) su FPR 2110. Il problema riguarda anche altre piattaforme hardware.
- Versione VDB corrente: 393. Sono interessate anche altre versioni del software.
- Versione VDB di destinazione: 427. Sono interessate anche altre versioni del software.

Risoluzione

Gli aggiornamenti VDB su FMC sono cumulativi e consentono aggiornamenti diretti da versioni

precedenti a versioni più recenti senza richiedere passaggi intermedi.

Processo di aggiornamento VDB

È possibile eseguire l'aggiornamento direttamente da VDB versione 393 a VDB versione 427 senza passaggi intermedi di aggiornamento di VDB. A partire dalla versione 357 di VDB, Cisco supporta l'installazione di qualsiasi versione di VDB a partire dal VDB di base sulla piattaforma FMC.

Per scaricare l'ultima versione di VDB, accedere all'Area download software Cisco all'indirizzo https://software.cisco.com/download/home/286332319/type/286321931/release/VDB

Considerazioni sull'impatto del servizio

Il rischio primario non è associato all'installazione VDB sul FMC, ma piuttosto alla prima distribuzione di criteri su FTD dopo l'aggiornamento del VDB. Nella maggior parte dei casi, la prima distribuzione dopo un aggiornamento VDB riavvia il processo Snort, che interrompe temporaneamente l'ispezione del traffico.

Durante questo periodo di interruzione:

- Il traffico può cadere o passare senza ulteriori ispezioni.
- Il comportamento specifico dipende dalla configurazione dell'FTD per la gestione del traffico durante il riavvio del processo.

Raccomandazioni sulle procedure ottimali:

- Pianificare la parte relativa alla distribuzione dei criteri durante un intervento di manutenzione pianificato.
- Coordinamento con le operazioni di rete per ridurre al minimo l'impatto sugli utenti.
- Monitorare lo stato del sistema durante e dopo il processo di distribuzione.

Causa

- A partire da VDB 357, è possibile installare qualsiasi aggiornamento di VDB a partire dal VDB di base per la console centrale.
- L'installazione richiede una ridistribuzione dei criteri per attivare le nuove firme di vulnerabilità, che attivano un riavvio del processo Snort sui dispositivi FTD gestiti. Questo riavvio determina una breve interruzione delle funzionalità di ispezione del traffico durante il caricamento del nuovo database e la reinizializzazione del motore di ispezione.

Contenuto correlato

- Guida all'amministrazione di Cisco Secure Firewall Management Center - Aggiornamenti del sistema
- Guida alla configurazione dei dispositivi di Cisco Secure Firewall Management Center - Distribuzione
- 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).