Vérifier les chemins de mise à jour directe VDB et l'impact du trafic sur FMC

Table des matières

Problème

Lorsqu'ils exécutent des mises à jour de base de données de failles (VDB), les administrateurs doivent déterminer si les mises à jour de base de données de failles sont cumulatives et s'ils peuvent ignorer les versions intermédiaires.

Dans cet exemple, la préoccupation concerne la mise à jour de la version 393 de VDB vers la version 427. Plus précisément, il existe une incertitude quant à la nécessité de plusieurs étapes de mise à niveau ou à la prise en charge d'un chemin de mise à niveau direct. En outre, des problèmes surviennent au sujet d'interruptions de service potentielles pendant la mise à jour de la VDB et le processus de déploiement de stratégie suivant.

Environnement

- Logiciel Secure Firewall Management Center (FMC) version 7.4.2.4. Les autres versions logicielles sont également affectées.
- Firewall Threat Defense (FTD) sur le document FPR 2110. D'autres plates-formes matérielles sont également concernées.
- Version VDB actuelle : 393. D'autres versions du logiciel sont également concernées.
- Version VDB cible : 427. D'autres versions de logiciels sont également concernées.

Résolution

Les mises à jour VDB sur FMC sont cumulatives, ce qui permet des mises à niveau directes des

versions plus anciennes vers les versions plus récentes sans nécessiter d'étapes intermédiaires.

Processus de mise à jour VDB

Vous pouvez mettre à jour directement de VDB version 393 vers VDB version 427 sans étapes intermédiaires de mise à niveau VDB. À partir de la version 357 de la VDB, Cisco prend en charge l'installation de toute version de la VDB jusqu'à la VDB de base sur la plate-forme FMC.

Pour télécharger la dernière version de VDB, consultez Téléchargement de logiciel.

Considérations sur l'impact

Le risque principal n'est pas associé à l'installation de la VDB elle-même sur le FMC, mais plutôt au premier déploiement de stratégie sur le FTD après la mise à jour de la VDB. Dans la plupart des cas, le premier déploiement après une mise à jour VDB redémarre le processus Snort, qui interrompt temporairement l'inspection du trafic.

Pendant cette période d'interruption :

- Le trafic peut être abandonné ou acheminé sans inspection supplémentaire.
- Le comportement spécifique dépend de la façon dont le FTD est configuré pour gérer le trafic pendant les redémarrages du processus.

Recommandations de meilleures pratiques :

- Planifier la partie déploiement de la stratégie pendant une fenêtre de maintenance planifiée.
- Coordination avec les opérations réseau pour minimiser l'impact sur les utilisateurs.
- Surveiller l'état du système pendant et après le processus de déploiement.

Motif

- À partir de VDB 357, vous pouvez installer toutes les mises à jour VDB jusqu'à la VDB de base pour le FMC.
- L'installation nécessite un redéploiement de stratégie pour activer les nouvelles signatures de vulnérabilité, ce qui déclenche un redémarrage du processus Snort sur les périphériques FTD gérés. Ce redémarrage entraîne une brève interruption des fonctionnalités d'inspection du trafic pendant le chargement de la nouvelle base de données et la réinitialisation du moteur d'inspection.

Autres informations utiles

- Guide d'administration de Cisco Secure Firewall Management Center - Mises à jour système
- Guide de configuration des périphériques Cisco Secure Firewall Management Center - Déploiement
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.