Dépannage des événements d'intrusion FMC indiquant Impact=Inconnu

Table des matières

Problème

Après le déploiement d'un nouveau Firewall Management Center (FMC) et la mise à niveau vers la version 7.7.12, tous les événements d'intrusion affichent « Impact=Unknown » au lieu des valeurs d'impact attendues. Cela empêche le déclenchement des mécanismes d'alerte appropriés, car le champ d'impact est requis pour la configuration des alertes.

Environnement

- FMC version 7.7.12. D’autres versions logicielles peuvent également être affectées.
- Stratégie d'intrusion en mode Prévention ou Détection.

Résolution

La résolution de ce problème implique la vérification et la configuration de la portée de la stratégie de détection pour inclure toutes les adresses IP pertinentes où des événements d'intrusion sont générés.

Étape 1 : identification des adresses IP affectées

Passez en revue les événements d'intrusion qui affichent « Impact=Unknown » et identifiez les adresses IP spécifiques impliquées dans ces événements. Documentez ces adresses IP à des

fins de comparaison avec la configuration actuelle de la stratégie de découverte.

Étape 2 : examen de la configuration actuelle de la stratégie de découverte

Accédez à Stratégies FMC > Découverte du réseau (dans les versions plus récentes, il s'agit de Stratégies > Avancé > Découverte du réseau) et examinez les paramètres de stratégie de découverte actuels pour déterminer quelles plages d'adresses IP ou quels sous-réseaux sont actuellement inclus dans l'étendue de la découverte.

Étape 3. Mise à jour du périmètre de la stratégie de découverte

Modifiez la configuration de la stratégie de détection pour inclure toutes les adresses IP où des événements d'intrusion se produisent. Assurez-vous que la portée de la stratégie de détection englobe tous les segments du réseau sur lesquels vous prévoyez de recevoir des événements d'intrusion avec une évaluation d'impact appropriée.

Étape 4. Déploiement des modifications de configuration

Déployez la configuration de stratégie de détection mise à jour sur tous les périphériques gérés pour garantir que les modifications prennent effet sur l'ensemble de l'infrastructure de sécurité.

Étape 5. Vérification du remplissage du champ d’impact

Surveillez les nouveaux événements d'intrusion pour confirmer que le champ d'impact est maintenant rempli avec les valeurs appropriées au lieu de « Inconnu ».

Motif

Les événements d'intrusion indiquant « Impact=Unknown » ont été provoqués par un problème de configuration où les adresses IP affectées n'étaient incluses dans aucune stratégie de détection sur le FMC. Lorsque les adresses IP ne sont pas couvertes par les stratégies de détection configurées, le FMC ne peut pas évaluer correctement l’impact des événements d’intrusion pour ces adresses, ce qui a pour conséquence que le champ d’impact est rempli avec des valeurs « Inconnues ». Il s'agit d'un problème de configuration plutôt que d'un défaut logiciel ou matériel.

Autres informations utiles

- Niveaux d'impact des événements d'intrusion
- 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.