Accès sécurisé Action d'avertissement Remplacer le comportement avec les paramètres de blocage IPS

Table des matières

Problème

Lorsque vous testez le comportement Avertir dans une stratégie d'accès (accès Internet) sur Cisco Secure Access avec IPS activé, les utilisateurs constatent un comportement inattendu où l'action Avertir semble remplacer les paramètres de blocage IPS. Plus précisément, lors de l'accès à une URL destinée à déclencher une signature IPS (tentative d'accès au fichier SERVER-WEBAPP /etc/passwd, GID-SID : 1-1122), une page d'avertissement s'affiche et après confirmation par l'utilisateur, l'accès à l'URL est autorisé malgré la configuration du système IPS pour bloquer le trafic.

La configuration inclut :

- Action : Isoler
- Prévention des intrusions (IPS) : Activer
- IPS / Bloquer
- Signature : SERVER-WEBAPP /etc/passwd tentative d'accès au fichier
- GID-SID : 1-1122

Les journaux de recherche d'activité affichent des entrées conflictuelles :

- IPS : (IPS : block)
- WEB : (WEB : autoriser - page d'avertissement affichée)
- WEB : (WEB : allow - after warning access)

Environnement

- Produit : Cisco Secure Internet Access Advantage
- Technologie : Accès sécurisé
- Stratégie d'accès configurée avec l'action Accès Internet et Avertissement
- IPS activé avec action de blocage pour des signatures spécifiques

Résolution

Ce comportement a été identifié comme un défaut dans Cisco Secure Access où l'action Avertir dans les stratégies d'accès a priorité sur les paramètres de blocage IPS. Le problème affecte l'interaction entre les actions d'avertissement de stratégie d'accès et la fonctionnalité de blocage IPS.

Étapes de vérification

Pour vérifier ce comportement dans votre environnement :

Étape 1: Configurez la stratégie d'accès avec l'action Avertir et activez le blocage IPS :

- Définissez Action sur Isoler avec le comportement Avertir.
- Activez la prévention des intrusions (IPS).
- Configurer IPS avec l'action Bloquer.
- Appliquez une signature spécifique (telle que SERVER-WEBAPP /etc/passwd, tentative d'accès au fichier, GID-SID : 1-1122).

Étape 2: Testez la configuration en accédant à une URL qui déclenche la signature IPS :

```
https://example.com/etc/passwd
```

Étape 3: Observez le comportement :

- La page d'avertissement s'affiche.
- L'utilisateur peut continuer après avoir confirmé l'avertissement.
- L'accès à l'URL est autorisé malgré la configuration du bloc IPS.

Étape 4: Vérifier les journaux de recherche d'activité :

- Vérifiez la présence d'entrées de bloc IPS et d'autorisation WEB.
- Confirmez que les entrées de journal en conflit indiquent le défaut.

État actuel

Ce comportement a été confirmé comme un défaut lorsque l'action Avertir remplace les paramètres de blocage IPS par conception dans l'implémentation actuelle. Le même comportement se produit avec les signatures IPS autres que GID-SID : 1-1122, indiquant qu'il s'agit d'un problème systémique affectant toutes les signatures IPS lorsque des actions Avertir sont configurées.

Un plan de correction et un calendrier pour ce défaut n'ont pas encore été déterminés. Les entreprises confrontées à ce problème doivent évaluer leurs stratégies de sécurité et envisager d'autres configurations si un blocage IPS strict est requis.

Motif

La cause principale est un défaut dans Cisco Secure Access où le traitement de l'action Avertir de la stratégie d'accès a priorité sur l'application du blocage IPS. Cette faille de conception permet aux utilisateurs de contourner les contrôles de sécurité IPS par le biais du mécanisme de confirmation d'avertissement, annulant ainsi la fonctionnalité de blocage IPS lorsque des actions d'avertissement sont configurées.

Autres informations utiles

- 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.