Contenu

Introduction

Cet article discute comment l'équipe de recherche de vulnérabilité (VRT) détermine l'état de règle dans des stratégies par défaut d'intrusion, et comment fait une appliance de Sourcefire déterminez l'état par défaut approprié pour une nouvelle règle.

Détermination d'état de règle dans une stratégie par défaut

Chaque règle a un champ de métadonnées, avec zéro valeurs de stratégie ou plus. Il y a actuellement six valeurs de stratégie possibles :

1. Sécurité-IPS de baisse
2. alerte Sécurité-IPS
3. équilibré-IPS de baisse
4. alerte équilibré-IPS
5. Connectivité-IPS de baisse
6. alerte Connectivité-IPS

Si une stratégie IPS est descendue par exemple du Sourcefire-fournissait la stratégie **équilibrée de Sécurité et de Connectivité**, le périphérique géré est en mode intégré, et une règle a une valeur de stratégie de métadonnées de la baisse équilibré-IPS, la règle sera placée pour relâcher et générer des événements dans votre stratégie IPS. Si une règle a une valeur de stratégie de la baisse seulement Sécurité-IPS, elle sera désactivée dans votre stratégie.

> Remarque: Si une règle a de plusieurs valeurs de stratégie spécifiées, par exemple : baisse Sécurité-IPS de stratégie, baisse équilibré-IPS de stratégie, il apparaît dans les deux stratégies. Si aucune valeur de stratégie n'est spécifiée pour une règle indiquée, elle apparaît dans aucune stratégies par défaut.

Si un périphérique géré est placé au mode passif, et une stratégie est placée pour chuter, ceci n'a aucun effet. Le périphérique génère simplement des alertes. Si un périphérique est sur le mode intégré, et une valeur de stratégie est placée pour chuter, la règle relâche des paquets par défaut. Si sa valeur de stratégie est placée pour alerter, elle génèrent seulement des événements, sans tomber.

En conclusion, dans la plupart des cas, si un paquet est lâché, une alerte est générée. C'est vrai à

moins que la suppression des alertes soit indépendamment configurée pour une règle donnée.

Comment fait Sourcefire déterminez un état par défaut approprié, pour une nouvelle règle

L'état par défaut d'une règle est basé sur un certain nombre de facteurs. Exemple :

Incidence

Choses à considérer

Combien est-il vraisemblablement que des tentatives seront faites pour exploiter cette vulnérabilité, et quel pourcentage de nos utilisateurs (les clients de Sourcefire et les plus larges reniflent-ils la communauté) est susceptible d'être vulnérable à cette vulnérabilité ?

Choses à se souvenir

Une vulnérabilité d'Internet Explorer avec des attaques connues a dans la nature beaucoup plus à haute impression que par exemple une fonction de base de données de SAP qui peut être utilisée avec malveillance quand des autorisations sont incorrectement configurées, ou une attaque par déni de service complexe dans un module obscur du kernel Linux. VRT fait un jugement d'incidence commençant par le score CVSS d'une vulnérabilité, l'ajustant selon les besoins avec n'importe quelles informations complémentaires que nous pouvons posséder. C'est la mesure la plus importante de tous, parce que nous activerons parfois une règle n'obtiendrions autrement pas activé/pour ne pas obtenir le positionnement pour relâcher si l'incidence est assez élevée.

Représentation

Choses à considérer

Attendons-nous cette règle d'être rapides ou lents sur un réseau « moyen » ?

Choses à se souvenir

Tandis que la vitesse d'une règle dépend entièrement du trafic qu'elle examine, qui rend la représentation difficile à mesurer, nous avons une idée générale de ce qui constitue un réseau normal, et de la façon dont une règle donnée exécute sur ce réseau normal. Nous savons également qu'une règle avec, par exemple, une correspondance satisfaite simple qui sont relativement longs (6 octets ou plus, typiquement) et relativement seul (c.-à-d. « obscureJavaScriptFunction() », et pas "|00 00 00 00|" ou « OBTIENNENT/HTTP/1.1") évaluera plus rapide qu'une règle avec un PCRE complexe, une gamme des clauses byte_test et/ou de byte_jump, etc. Avec cette connaissance nous pouvons déterminer si une règle sera rapide ou lente et prend en compte cela.

Confiance

Choses à considérer

Combien est vraisemblablement cette règle de générer des faux positifs ?

Choses à se souvenir

Quelques vulnérabilités exigent des conditions très spécifiques et facilement détectées d'être présentes afin de pour être exploitées, dans ce cas nous pouvons être très sûrs que n'importe quand la règle associée se déclenche, une exploit vivante est en cours. Par exemple, s'il y a un débordement de tampon dans un protocole qui a une seule chaîne magique à un à position fixe, et puis une longueur spécifiée qui est une distance fixe à partir de cette chaîne magique, nous pouvons être sûrs dans notre capacité de trouver la chaîne magique et de la vérifier contre une valeur connue pour des problèmes. Dans d'autres cas, les problèmes sont beaucoup moins bien définis ; par exemple, certaines attaques d'empoisonnement de cache DNS peuvent être indiquées par un nombre anormalement grand de réponses NXDOMAIN provenant un serveur dans une certaine période. En pareil cas, la simple présence d'une réponse NXDOMAIN n'est pas seule un indicateur d'une exploit ; c'est la présence d'un très grand nombre de telles réponses en peu de temps qui indique le problème. Puisque ce nombre sera différent pour différents réseaux, le VRT est forcé pour choisir une valeur qui devrait fonctionner pour la plupart des réseaux et libérer cela ; cependant, nous ne pouvons pas être 100% sûr cela, quand la règle se déclenche, action malveillante réelle se produit.

Àenfin et surtout, alors que d'autres facteurs peuvent être considérés de temps en temps comme appropriés, l'incidence est roi finalement - veillant nos clients sont protégés contre les menaces il est le plus susceptible les voir que dans la nature est notre principale préoccupation.