Contenu

Introduction

La mise à jour de règle de Sourcefire de releases de l'équipe de recherche de vulnérabilité (VRT) (SRU) pour adresser les dernières menaces et vulnérabilités. Une nouvelle release SRU peut contenir la stratégie de base mise à jour pour l'usage à une installation de renifler. Ce document explique le processus utilisé par l'équipe de recherche de vulnérabilité pour décider comment des règles sont assignées à chaque stratégie.

Mesures utilisées pour déterminer Ruleset par défaut

- La mesure principale utilisée est le score commun du système de notation de vulnérabilité (CVSS) assigné à chaque vulnérabilité qui pourrait être couverte par une règle.
- La deuxième mesure est basé temporel et concerne l'âge d'une vulnérabilité particulière.
- La mesure finale est la zone de la couverture particulière pour la règle. Tellement par exemple, des règles d'injection SQL sont considérées assez importantes pour avoir l'influence en étant considéré pour l'intégration de stratégie.

  Remarque: Les vulnérabilités couvertes par les règles dans ces catégories sont considérées importantes, indépendamment de l'âge.

Connectivité au-dessus de stratégie de base de Sécurité

1. Le score CVSS doit être 10

2. Âge de la vulnérabilité

   - Année en cours (2014 par exemple)
   - L'année dernière (2013 dans cet exemple)
   - Année avant le bout (2012 dans cet exemple)
3. Catégorie de règle

   - Non utilisé pour cette stratégie

Stratégie de base équilibrée

Remarque: La stratégie **équilibrée** est l'état par défaut d'expédition du VRT Ruleset pour Open Source reniflent.

1. Score 9 CVSS ou plus grand

2. Âge de la vulnérabilité

   - Année en cours (2014 par exemple)
   - L'année dernière (2013 dans cet exemple)
   - Année avant le bout (2012 dans cet exemple)

3. Catégorie de règle

   - Malware-commande numérique par ordinateur
   - Liste noire
   - Injection SQL
   - Exploit-kit

Sécurité au-dessus de stratégie de base de Connectivité

1. Score 8 CVSS ou plus grand

2. Âge de la vulnérabilité

   - Année en cours (2014 par exemple)
   - L'année dernière (2013 dans cet exemple)
   - Année avant le bout (2012 dans cet exemple)
   - Année antérieurement (2011 dans cet exemple)

3. Catégorie de règle

   - Malware-commande numérique par ordinateur
   - Liste noire
   - Injection SQL
   - Exploit-kit
   - App-le détectez

Fréquence des mises à jour de stratégie

Toutes les nouvelles règles sont placées dans un ou plusieurs des stratégies de base basées sur les critères identifiés. Les stratégies sont réévaluées chaque année, et des règles des années précédentes, pendant que les vulnérabilités vieillissent, sont retirées d'une stratégie pour maintenir la stratégie conforme avec les critères de sélection.

Si les règles se déplacent entre les catégories, leur présence dans les stratégies sont également décidées basée sur le processus de sélection de catégorie. De même, la modification de score CVSS pour une vulnérabilité particulière qui est couverte par une règle, c'est présence dans une stratégie basée sur la mesure CVSS est également réévalué.

Remarque: Des règles dans les stratégies énumérées sont évaluées sur une règle par base de règle. Il y aura quelques règles qui sont plus anciennes et pas dans les critères au-dessus de cela soyez dans les stratégies par défaut. Ce qui précède est les critères de sélection pour des règles par défaut, et est sujet toujours à la modification basée sur l'horizontal de menace.