目次

概要

最新の脅威および脆弱性に対処する脆弱性調査チーム（VRT）リリース Sourcefire ルール アップデート（SRU）。 新しい SRU リリースは Snort インストールで使用のための更新済基礎ポリシーが含まれているかもしれません。 この資料はルールが各ポリシーにどのように割り当てられるか決定するために脆弱性調査チームが使用するプロセスを説明したものです。

デフォルト Ruleset を判別するのに使用されるメトリック

- 使用される主要なメトリックはルールによってカバーされるかもしれない各脆弱性に割り当てられるよくある脆弱性採点法（CVSS）スコアです。
- 第 2 メトリックは一時的な基づいて、特定の脆弱性の経過時間にかかわります。
- 最終的なメトリックはルールのためのカバレッジの特定の工リアです。 そうたとえば、SQL インジェクション ルールは効力を持つには十分に重要であるために考えられときポリシー包含のために考慮されます。

  注: これらのカテゴリーのルールによってカバーされる脆弱性は、経過時間に関係なく重要考慮されます。

安全ベース ポリシー上の接続

1. CVSSスコアは 10 である必要があります

2. 脆弱性の経過時間

   - 今年（2014 たとえば）
   - 昨年（この例の 2013）
   - 最後（この例の 2012）の前の年

3. ルール カテゴリ

   - このポリシーのために使用されなくて

平衡型基礎ポリシー

注: 平衡型ポリシーはオープン ソース Snort のための VRT Ruleset のデフォルト配布状態です。

1. CVSSスコア 9 またはより大きい

2. 脆弱性の経過時間

   - 今年 (2014 たとえば)
   - 昨年 (この例の 2013)
   - 最後 (この例の 2012) の前の年
3. ルール カテゴリ

   - Malware CNC
   - ブラックリスト
   - SQL インジェクション
   - エクスプロイト キット

接続ベース ポリシー上のセキュリティ

1. CVSSスコア 8 またはより大きい

2. 脆弱性の経過時間

   - 今年 (2014 たとえば)
   - 昨年 (この例の 2013)
   - 最後 (この例の 2012) の前の年
   - 前の年 (この例の 2011)
3. ルール カテゴリ

   - Malware CNC
   - ブラックリスト
   - SQL インジェクション
   - エクスプロイト キット
   - アプリケーション検出

ポリシー更新の周波数

すべての新しいルールは識別された基準に基づいて基礎ポリシーの何れか一つ以上に置かれます。 ポリシーは毎年再査定され、ポリシーを選択基準と対応保存するために脆弱性が老化すると同時に、前年からのルールはポリシーから取除かれます。

ルールがカテゴリーの間で移動する場合、ポリシーの存在はまたカテゴリ 選択過程に基づいて決定されます。 同様にルールによってカバーされる特定の脆弱性のための CVSS スコア変更が、また CVSS メトリックに基づいてポリシーの存在再査定されますです。

注: リストされたポリシーのルールはルール基礎によってルールで評価されます。 より古いないそれの上の基準でデフォルトポリシーにあって下さいいくつかのルールがあり。 上は

デフォルトのルールのための選択基準で、脅威状況に基づいて変更に応じて常にあります。