目次

概要

この技術情報は脆弱性調査チーム（VRT）がデフォルト不正侵入ポリシーのルール状態をどのように判別する、および Sourcefire アプライアンスをどのようにするか新しいルールのための適切な既定値状態を判別して下さいか論議します。

デフォルトポリシーのルール状態の判断

各ルールにゼロありますまたはより多くのポリシー値を用いるメタデータ フィールドが。 現在 6 つの可能性のあるポリシー値があります:

1. セキュリティ IPS ドロップする
2. セキュリティ IPS アラート
3. 平衡型 IPS ドロップする
4. 平衡型 IPS アラート
5. 接続 IPS ドロップする
6. 接続 IPS アラート

IPS ポリシーがから Sourcefire 提供したら**平衡型セキュリティおよび接続** ポリシーを降りる場合、管理対象装置はインライン モードにあり、ルールに平衡型 IPS ドロップするのメタデータ ポリシー値があります IPS ポリシーのイベントを廃棄し、生成する、ルールは設定 されます。 ルールにセキュリティ IPS ドロップするだけのポリシー値がある場合、ポリシーでディセーブルにされます。

> **注** ルールに規定 される 複数のポリシー値がある場合たとえば: ポリシー セキュリティ IPS ドロップする、ポリシー平衡型 IPS ドロップする、それは両方のポリシーに現われます。 ポリシー値がある特定のルールのために規定 されない場合、ポリシーにデフォルトで現われません。

管理対象装置がパッシブモードに設定 され、ポリシーが廃棄するために設定 されれば場合これは効果をもたらしません。 デバイスはアラートを単に生成します。 デバイスがインライン モードにあり、ポリシー値が廃棄するために設定 されれば場合ルールはパケットをデフォルトで廃棄します。 ポリシー値が警告 するために設定 される場合それ廃棄しないで生成する イベントだけ。

最終的にはパケットが廃棄されれば、ほとんどの場合、アラートは生成されます。 これはアラートの抑制がある特定のルールのために独自に設定されなければ本当です。

Sourcefire をどのようにするか新しいルールのための適切な既定値状態を、判別して下さい

ルールのデフォルトステートはいくつかのファクタに基づいています。 次に、例を示します。

影響

考慮するべき事柄

どの程度その試み作りますこの脆弱性を不正利用することをでありこの脆弱性に脆弱である何パーセントのユーザ（Sourcefire 両方顧客およびより広い Snort コミュニティ）が可能性が高いですか。

覚えるべき事柄

権限が不適当に設定される、または複雑なサービス拒否攻撃できるとき野生の既知の攻撃を用いる Internet Explorer 脆弱性に Linuxカーネルの曖昧なモジュールで悪意をもって使用 SAP データベース関数がより大いに影響が大きくあります。 VRT は所有するかもしれないあらゆるその他の情報で必要に応じてそれを調節する脆弱性の CVSS スコアから開始する影響判断をします。 これは影響が十分に高くある場合セットを得ないように時々廃棄するためにルールを他では得る回された/有効に するので、すべての最も重要なメトリックです。

パフォーマンス

考慮するべき事柄

「平均」ネットワークでファーストまたは遅いこのルールを期待しますか。

覚えるべき事柄

ルールの速度がパフォーマンスを測定すること困難にする、検査しているトラフィックに完全に依存している間、正常なネットワークを構成するものが、そしてある特定のルール実行するどのようにのその正常なネットワークで一般的な考えがあります。 および比較的ユニークことをルールがとの、たとえば、比較的長い（単一コンテンツ一致 6 のまたはより多くのバイト、一般的に）（すなわち「obscureJavaScriptFunction()」、およびない "|00 00 00 00|" または「GET/HTTP/1.1" ）複雑な PCRE、一連の byte_test および/または byte_jump 句とのルールより速く評価しますこともまた、先祖など確認します このナレッジを使うとルールがファーストまたは遅かった、考慮事項にそれを運ぶかどうか確認できます。

信任

考慮するべき事柄

どの程度 false positive を生成するこのルールはありますか。

覚えるべき事柄

いくつかの脆弱性はいつでも関連するルールが起動 する非常に確信します不正利用されるためにあるために極めて特殊な、容易に検出する状態、ライブ エクスプロイトです進行中必要となります。 たとえば次に固定位置でユニークな魔法ストリングがある、その魔法ストリングからの固定距離である指定された長さ、魔法ストリングを検索し、問題に関しては既知の値に対してチェックする機能で確信しプロトコルにバッファオーバーフローがあれば。 それ以外の場合、問題は大いにより少なく明示されています; たとえば、不正侵入の毒するある特定の DNS キャッシュはによって大きな 番号ある特定のある一定の時間のサーバから来る NXDOMAIN 応答の異常に示すことができます。 このような場合、NXDOMAIN 応答のただの存在はそれ自体エクスプロイトのインジケータではないです; 問題を示唆する非常に多くのそのような応答の近いうちにのは存在です。 その数が異なるネットワークのために異なっているのでほとんどのネットワークのためにはたらき、それをリリースする必要がある値を選択するために、VRT は強制されます; ただしルールが起動 するとき、それ、実際の悪意のあるアクティビティ発生しています確信した 100% オである場合もありません。

大事なことを言い忘れたがで、他のファクタは関連したように時々考慮されるかもしれないが影響は結局は王です-確かめて顧客はによって野生で見る可能性が高いである最大の関心事脅威から保護されます。