IIS 4.0 および 5．0 の Microsoft インデックス サーバ ISAPI 拡張における「Code Red」ワームのリモート バッファ オーバーフローに対する シスコ Secure IDS/Netranger カスタム ストリング照合型シグニチャの使用

目次

概要

Computer Economics 社（カリフォルニア州 Carlsbad の独立系調査組織）は 2003 年 7 月末現在、「Code Red」ワームが原因で企業にネットワークの損害の回復や生産性の損失などにかかったコストは、12 億 US ドルにのぼると推定しています。 推定額は、最近より強力な「Code Red II」ワームがリリースされたことにより、大幅に増加するとみられます。 Cisco SAFE Blueprint の主要コンポーネントである Cisco Secure Intrusion Detection System（IDS; セキュア侵入検知システム）は、「Code Red」ワームをはじめとするネットワーク セキュリティのリスクを検知し、これを軽減するという価値を証明してきました。

この文書では、「Code Red」ワームが使用する不正利用方式（下記のシグニチャ 2 を参照）を検知するソフトウェア アップデートについて説明します。

次のカスタム ストリング照合型シグニチャを作成すると、Microsoft Windows NT と Internet Information Services（IIS）4.0 または Windows 2000 と IIS 5.0 を実行している Web サーバに対し、バッファ オーバーフローの不正利用を捕捉することができます。 また、Windows XP ベータのインデックス サービスも脆弱であることにも注意してください。 この脆弱性を記述する Security Advisory は http://www.eeye.com/html/Research/Advisories/AD20010618.html にあります。 Microsoft は http://www.microsoft.com/technet/security/bulletin/MS01-033.mspx からダウンロードすることができるこの脆弱性のためのパッチをリリースしました。

この資料で説明されていたシグニチャはシグニチャアップデート リリース S(5) で利用可能になりました。 シスコシステムズは、このシグニチャを実装する前に、センサーを 2.2.1.8 または

2.5(1)S3 シグニチャ アップデートにアップグレードすることを推奨しています。 登録ユーザは Cisco セキュア ソフトウェア センターからこれらのシグニチャアップデートをダウンロードできます。 どのユーザでも、「Cisco Worldwide Contacts」に掲載されている連絡先に電子メールを送信、および電話することで、Cisco Technical Support に連絡できます。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

この設定は、次のバージョンのソフトウェアおよびハードウェアを使用して作成と動作確認が行われました。

- Microsoft Windows NT および IIS 4.0
- Microsoft Windows 2000 および IIS 5.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

カスタム ストリング照合シグニチャ

この問題に対処するための、特定のカスタム ストリング照合型シグニチャが 2 種類あります。各シグニチャについて次に説明します。また、適用可能な製品設定についても説明します。

シグニチャ 1 不正利用目的によるインデックス サーバへのアクセスの試み

このシグニチャは、シェルコードをサーバへ送り、コードの元の形態で特権アクセスを取得しようとする動きに対処すると同時に、Indexing Server ISAPI Extension へのバッファ オーバーフローの不正利用に対処するためのものです。 このシグニチャは、シェルコードをターゲットとなるサービスへ送り、完全なシステム レベルのアクセスを取得しようとする攻撃にのみ対処します。ここで考えられる問題は、このシグニチャは、アタッカーがシェルコードを送ろうとせずに、IIS をクラッシュさせてサービスを拒否状態にするため、サービスに対してバッファ オーバーフローだけを実行する攻撃に対しては対処しないことです。

String

```
[Gg][Ee][Tt].*[.][Ii][Dd][Aa][\x00-\x7f]+[\x80-\xff]
```

製品設定

- 発生： 1

- Port: 80

注: 別のTCP ポート（8080 など）を受信している Web サーバが存在する場合、ポート番号ごとに個別のカスタム ストリング照合型を作成する必要があります。

- 推奨されるアラーム重要度高い（Cisco Secure Policy Manager）5（Unix 管理者）
- [Direction]：『

シグニチャ 2 -「Code Red」ワームによるインデックス サーバ アクセス バッファ オーバーフロー

2 番目のシグニチャは、シェルコードをサーバへ送り、"Code Red" ワームで使用される不明瞭な形態で特権アクセスを取得しようとする動きに対処すると同時に、Indexing Server ISAPI Extension のバッファ オーバーフローの不正利用に対処するためのものです。 このシグニチャは、シェルコードをターゲットとなるサービスへ送り、完全なシステム レベルのアクセスを取得しようする攻撃にのみ対処します。 ここで考えられる問題は、このシグニチャは、アタッカーがシェルコードを送ろうとせずに、IIS をクラッシュさせてサービスを拒否状態にするため、サービスに対してバッファ オーバーフローだけを実行する攻撃に対しては対処しないことです。

String

```
[/]default[.]ida[?][a-zA-Z0-9]+%u
```

注: 上記ストリングには、スペースを挿入しません。

製品設定

- 発生： 1
- Port: 80

注: 別のTCP ポート（8080 など）を受信している Web サーバが存在する場合、ポート番号ごとに個別のカスタム ストリング照合型を作成する必要があります。

- 推奨されるアラーム重要度高い（Cisco Secure Policy Manager）5（Unix 管理者）
- [Direction]：『

on Cisco Secure IDS 詳細については、Cisco Secure Intrusion Detection を参照して下さい。

関連情報

- テクニカル サポート：ルータ
- Cisco セキュリティ アドバイザリ
- Cisco Secure Intrusion Detection のサポートページ
- テクニカルサポート - Cisco Systems