Cisco Secure Intrusion Detection System の署名の難読化に関する脆弱性

severity

アドバイザリーID : cisco-sa-20010906-intrusion-detection

初公開日 : 2001-09-06 00:00

バージョン 1.5 : Final

回避策 : Yes

Cisco バグ ID :

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

容疑者または悪質なパケット 形式、データペイロードおよびトラフィックパターンのための Intrusion Detection Systems Inspect ネットワークトラフィック。 一般的に Intrusion Detection Systems 実装する不明化防御-容疑者パケットが UTF や 16進 エンコーディングと容易に隠れ、Intrusion Detection Systems をバイパスできないようにします。 最近、CodeRed ワームは Microsoft 多くの IIS システムとのパッチ設定されていない脆弱性を目標とし、また Microsoft IIS システムによってサポートされる別のエンコード技術を強調表示しました。 %u として知られているこのエンコード技術が Intrusion Detection Systems を避けるのに使用することができ http://www.eeye.com/html/Research/Advisories/AD20010705.html にある発表の eEye セキュリティによって公共に作られました 。

Cisco は以前顧客に現在利用可能であるサービスパックとの Netranger として、知られている Cisco Secure Intrusion Detection System のこの脆弱性を、解決しました。 この脆弱性はまた Cisco Catalyst 6000 Intrusion Detection System Module に影響を与え、2002 年 5 月にリリースされるリリース 3.0(4)S20 で修理されます。 Cisco はこのアドバイザリの Workaround セクションにリストされているこの問題に回避策を提供しました。

完全な表記は http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010906-intrusion-detection で利用できます。

該当製品

修正済みソフトウェア

以下の製品は影響を受けています:

- 以前 NetRanger として知られている Cisco Secure Intrusion Detection System、センサー コンポーネント
- Cisco Catalyst 6000 Intrusion Detection System Module

すべての可能性のために明確に設定されてさらに、NBAR の使用のような指定回避策、か Cisco Cache Engine、なぜなら CodeRed ワーム エクスプロイトをフィルタリングすることは %u エンコード攻撃不明化を検出する。

脆弱性を含んでいないことが確認された製品

Unix および NT 両方プラットフォームのための Cisco Secure Intrusion Detection System ディレクターは IDS の管理コンポーネントで、パケット 難読化 の 検出に加わらないし、この脆弱性から影響を受けません。

以下の製品は侵入検知 攻撃 シグニチャの限定サブセットが実装され、従って含まれているシグニチャは Microsoft IIS によって目標とされる不正侵入を検出するし、攻撃不明化の %u 符号化 方式に脆弱です。

- Cisco Secure PIX Firewall
- 侵入検知を用いる Cisco IOS ファイアウォール機能セット

他のシスコ製品においてこのアドバイザリの影響を受けるものは、現在確認されていません。

改訂履歴

Revision 1.5	24 年 JAN 月 2003 日	ソフトウェア バージョン および 修正 セクションからの取除かれたベータコード情報および位置。
リビジョン 1.4	2002-SEP-27	更新済要約、詳細、ソフトウェア バージョン および 修正およびこの通知 の ステータス。
リビジョン 1.3	2001-OCT-17	ソフトウェア バージョンの更新済詳細及び修正およびこの通知 の ステータス。
リビジョン 1.2	2001-SEP-27	修正済みソフトウェアを入手するための手順の更新済詳細。
リビジョン 1.1	2001-SEP-14	回避策の更新済詳細および修正済みソフトウェアを入手するための手順。
リビジョン	2001-SEP-05	初回公開リリース

1.0		

利用規約

本アドバイザリは無保証のものとしてご提供しており、いかなる種類の保証も示唆するものではありません。 本アドバイザリの情報およびリンクの使用に関する責任の一切はそれらの使用者にあるものとします。 また、シスコは本ドキュメントの内容を予告なしに変更したり、更新したりする権利を有します。
本アドバイザリの記述内容に関して情報配信の URL を省略し、単独の転載や意訳を施した場合、当社が管理した情報とは見なされません。そうした情報は、事実誤認を引き起こしたり、重要な情報が欠落していたりする可能性があります。 このドキュメントの情報は、シスコ製品のエンドユーザを対象としています。