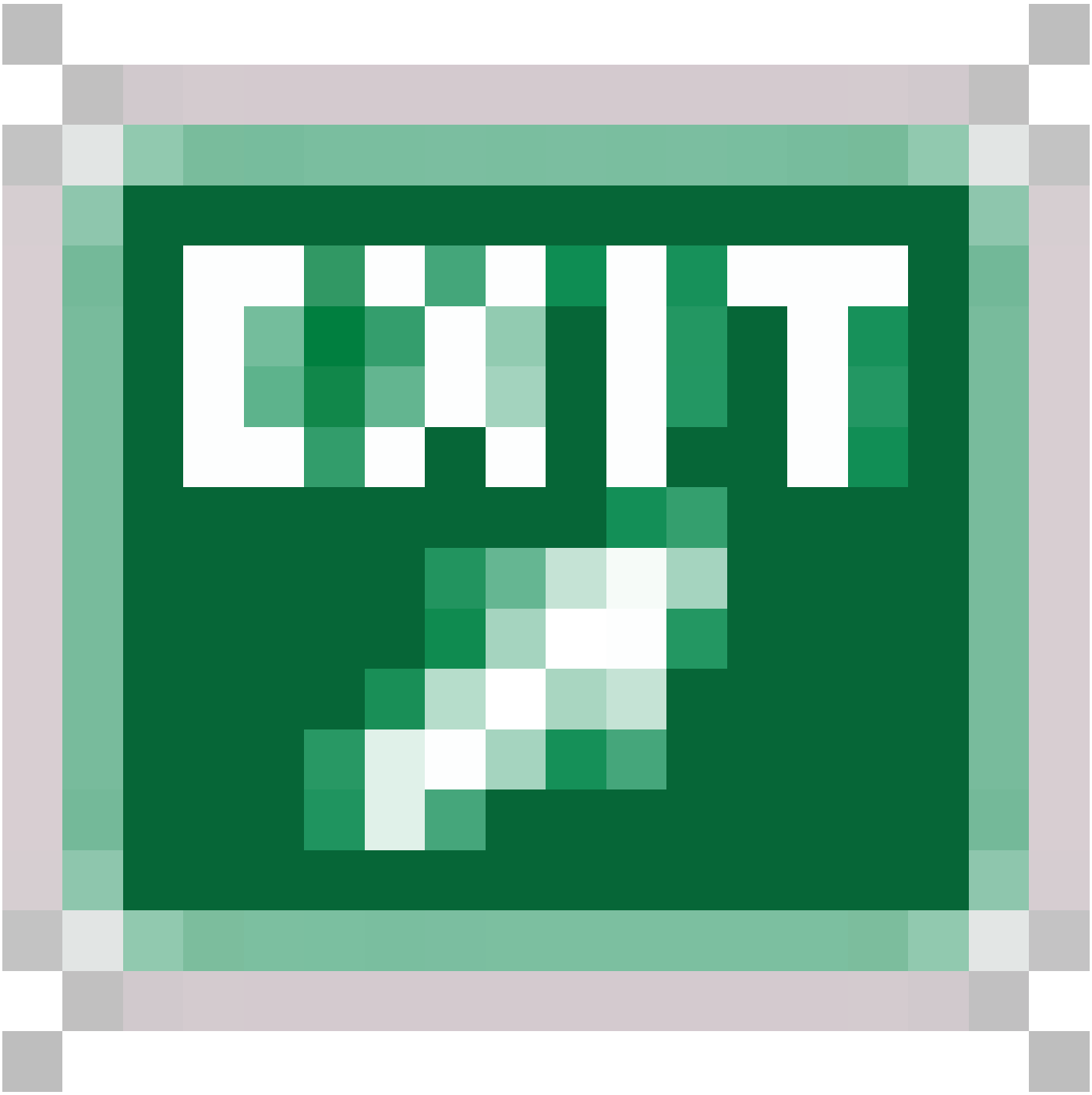
Cisco Secure Intrusion Detection System の署名の難読化に関する脆弱性

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 : No Workarounds available
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

Intrusion Detection System（IDS；侵入検知システム）は、疑わしいパケット形式や悪意のあるパケット形式、データペイロード、トラフィックパターンがないか、ネットワークトラフィックを検査します。侵入検知システムは通常、難読化防御を実装します。これにより、疑わしいパケットがUTFや16進数のエンコードで簡単に偽装され、侵入検知システムをバイパスすることを防ぎます。最近、CodeRedワームは、多くのMicroSoft IISシステムに対するパッチ未適用の脆弱性を標的にしており、MicroSoft IISシステムでサポートされている別の符号化技術も強調しています。%uと呼ばれるこの符号化技術は、侵入検知システムを回避するために使用でき、http://www.eeye.com/html/Research/Advisories/AD20010705.htmlにあるeEye securityのアナウンスで公開されてい



ます。

シスコでは、Cisco Secure Intrusion Detection System(IDS)（旧Netranger）のこの脆弱性を、お客様が利用できるサービスパックで修正しました。この脆弱性は、Cisco Catalyst 6000 Intrusion Detection System Moduleにも影響を与え、2002年5月にリリースされたリリース3.0(4)S20で修復されています。シスコはこの問題の回避策を提供しています。この回避策は、このアドバイザリの「回避策」セクションに記載されています。

完全な通知は、
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010906-intrusion-detectionで入手できます。

該当製品

このセクションには、該当製品に関する詳細が掲載されています。

脆弱性のある製品

次の製品が影響を受けます。

- Cisco Secure Intrusion Detection System(IDS)（旧称NetRanger、センサーコンポーネント）
- Cisco Catalyst 6000 Intrusion Detection Systemモジュール

また、NBARやCisco Cache Engineを使用してCodeRedワームをフィルタリングするなどの回避策を講じた場合、可能な限り明示的に設定しない限り、%uエンコーディング攻撃の難読化は検出されません。

脆弱性を含んでいないことが確認された製品

UnixプラットフォームおよびNTプラットフォームの両方のCisco Secure Intrusion Detection System DirectorはIDSの管理コンポーネントであり、パケット難読化検出には関与しないため、この脆弱性の影響を受けません。

次の製品は、侵入検知攻撃シグニチャの限定されたサブセットを実装しており、含まれているシグニチャはMicroSoft IISターゲット攻撃を検出しないため、攻撃を不明化する%uエンコード方式に対して脆弱ではありません。

- Cisco Secure PIXファイアウォール
- 侵入検知を備えたCisco IOS Firewallフィーチャセット

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。

詳細

「CodeRed」ワームは、不明瞭なUnicode符号化技術を使用してワームのペイロードを配信しました。%uエンコード方式は、IIS Webサーバーによって認識および解析される別のエンコード方式です。このエンコーディングをurlの他の部分に適用して、攻撃を効果的に難読化し、利用可能な多くの侵入検知システムによる検出を防ぐことができます。Cisco Secure Intrusion Detection System(IDS)Sensorのデコードアルゴリズムは、このUnicode形式を検出して解析するように変更されています。Cisco Catalyst 6000 Intrusion Detection Systems（IDS；侵入検知システム）モジュールでは、この通知の最初の掲載時には難読化の検出は実装されていませんでしたが、2002年5月の時点でこの機能が含まれています。

この脆弱性は、Cisco Bug ID CSCdv20287に記載されています。この脆弱性は、Miter CVEでもCAN-2001-0669としてリストされています。

回避策

この問題には、Cisco Secure Intrusion Detection System SensorとCatalyst 6000 Intrusion Detection System Moduleの両方に対する回避策があります。

カスタム文字列照合シグニチャは、%u unicode難読化の脆弱性に対処するように定義できます。

このカスタムストリング照合は、Unicode難読化の使用を検出します。ユニコード文字列の正当な使用は、我々が気付かない可能性があるため、このシグニチャは正当なトラフィックパターンで警告する可能性があります。このシグニチャには、関連するアラームを注意深く監視する必要があります。

```
Signature 1
****************************************
Unicode Obfuscation String:
"[%][uU][0-9a-FA-F][0-9a-fA-F][0-9a-fA-F][0-9a-fA-F]"
Occurrences:
1
Port:
80
If you have Web servers listening on other TCP ports (for example, 8080), you will
need to create a separate custom string match for each port number.
Recommended Alarm Severity Level:
High (CSPM)
5 (Unix Director)
Direction:
TO
************************************************************
```

カスタムストリングマッチ機能の詳細については、http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csids/csids5/csidscog/で入手可能なドキュメントを参照してください。

修正済みソフトウェア

この脆弱性は、Cisco Secure Intrusion Detection System Sensorのサービスパック3.0(2)S6で修正され、今後すべてのバージョンに含まれる予定です。

この脆弱性は、Cisco Catalyst 6000 Intrusion Detection Moduleのサービスパック3.0で修正される予定です。基本的な難読化の検出は、当初は3.0リリースで予定されていましたが、2001年10月上旬にリリースされる予定です。3.0リリースのサービスパックには、この追加の難読化方式が含まれますが、2001年10月のリリース以降は使用できなくなります。このサービスパックリリースは3.0(4)S20で、2002年5月現在で利用可能です。

推奨事項

$propertyAndFields.get("recommendations")

不正利用事例と公式発表

この脆弱性はeEyeセキュリティチームによって発表され、eEyeセキュリティサイト

(http://www.eeye.com/html/Research/Advisories/AD20010705.html)で公開されています。

シスコでは、この不明化手法のエクスプロイトに関する知識を持っていません。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20010906-intrusion-detection

改訂履歴

Revision 1.5	2003年1月24日	「ソフトウェアバージョンと修正」セクションからベータコード情報と場所を削除。
リビジョン 1.4	2002年9月27日	この通知の概要、詳細、ソフトウェアバージョンと修正、およびステータスを更新。
リビジョン 1.3	2001-OCT-17	ソフトウェアバージョンと修正の詳細、およびこの通知のステータスを更新。
リビジョン 1.2	2001年9月27日	修正済みソフトウェアの入手手順の詳細を更新。
リビジョン 1.1	2001年9月14日	修正済みソフトウェアを入手するための回避策と手順の詳細を更新。

リビジョン 1.0	2001年9月5日	初回公開リリース

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。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。