

Cisco Security Agent および MS07-014 (Microsoft Word) の脆弱性により、リモートでコードが実行される問題 (929434)

概要

2007年2月13日、Microsoft Word アプリケーション (Microsoft Office 2000、Office XP、Office 2003、Microsoft Works Suite) に重大な脆弱性があることが発表されました¹。この脆弱性は現在、頻繁に悪用されています。リモートでコードが実行される脆弱性を攻撃者が悪用すると、影響を受けるシステムが完全に制御される可能性があります。Microsoft 社は、アップデート ファイルを提供し、影響を受けたシステムにパッチを早急に適用するよう推奨しています。

この脆弱性を悪用したさまざまな攻撃がすでに出回っています。シスコシステムズはエクスプロイト ファイルを入手し、Cisco Security Agent でデフォルトのセキュリティ ポリシー設定を使用することで、これらのエクスプロイトを阻止する効果があることを確認しました。現在サポート中のバージョンである Cisco Security Agent 4.0.3.x、4.5.1.x、5.0.0.x、および 5.1.0.x は、今までに確認されているエクスプロイトを防ぐうえで効果的です。

脆弱性の詳細情報

ユーザが管理ユーザ権限でログインした場合、以下の脆弱性を悪用する攻撃者によって、影響を受けるシステムが完全に制御される可能性があります。攻撃者はその後、プログラムのインストール、データの閲覧/変更/削除、完全なユーザ権限を持つ新規アカウントの作成などを実行できます。

Word の不正な形式の文字列の脆弱性 — CVE-2006-5994

Microsoft Word が特別に細工された文字列を持つ Word ファイルを処理する方法に、リモートでコードが実行される脆弱性が存在します。このような特別に細工されたファイルは、Eメールの添付ファイルに含まれているか、悪意のある Web サイトにホストされている可能性があります。特別に細工された Word ファイルを攻撃者が作成することにより、この脆弱性が悪用されてリモートでコードが実行される可能性があります。

Word の不正な形式のデータの構造の脆弱性 — CVE-2006-6456

特別に細工されたデータ構造を持つ Word ファイルを Microsoft Word が処理する方法に、リモートでコードが実行される脆弱性が存在します。このような特別に細工されたファイルは、Eメールの添付ファイルに含まれているか、悪意のある Web サイトにホストされている可能性があります。特別に細工された Word ファイルを攻撃者が作成することにより、この脆弱性が悪用されてリモートでコードが実行される可能性があります。影響を受ける Outlook のバージョンで不正な形式の Eメール メッセージを表示またはプレビュー表示することによって、この脆弱性が悪用されることはありません。

Word カウントの脆弱性 — CVE-2006-6561

Microsoft Word にリモートでコードが実行される脆弱性が存在します。Word がファイルを解析し、未チェックのカウントを処理する際に、この脆弱性が悪用される可能性があります。このような特別に細工されたファイルは、Eメールの添付ファイルに含まれているか、悪意のある Web サイトにホ

¹ Microsoft: <http://www.microsoft.com/technet/security/Bulletin/MS07-014.msp>

ストされている可能性があります。特別に細工された Word ファイルを攻撃者が作成することにより、この脆弱性が悪用されてリモートでコードが実行される可能性があります。影響を受ける Outlook のバージョンで不正な形式の E メール メッセージを表示またはプレビュー表示することによって、この脆弱性が悪用されることはありません。

Word マクロの脆弱性 — CVE-2007-0208

Microsoft Word にリモートでコードが実行される脆弱性が存在します。ユーザが管理ユーザ権限でログインした場合、この脆弱性を悪用する攻撃者によって、影響を受けるシステムが完全に制御される可能性があります。攻撃者はその後、プログラムのインストール、データの閲覧/変更/削除、完全なユーザ権限を持つ新規アカウントの作成などを実行できます。システム上で少ないユーザ権限しか持たないように設定されたアカウントのユーザは、管理ユーザ権限で実行するユーザと比べ、受ける影響は少なくなります。

Word の不正な形式の描画オブジェクトの脆弱性 — CVE-2007-0209

Microsoft Word にリモートでコードが実行される脆弱性が存在します。Word がファイルを解析し、不正な形式の描画オブジェクトを処理する際に、この脆弱性が悪用される可能性があります。このような特別に細工されたファイルは、Eメールの添付ファイルに含まれているか、悪意のある Web サイトにホストされている可能性があります。特別に細工された Word ファイルを攻撃者が作成することにより、この脆弱性が悪用されてリモートでコードが実行される可能性があります。

Word の不正な形式の機能の脆弱性 — CVE-2007-0515

Microsoft Word にリモートでコードが実行される脆弱性が存在します。Word がファイルを解析し、不正な形式の機能を処理する際に、この脆弱性が悪用される可能性があります。このような特別に細工されたファイルは、Eメールの添付ファイルに含まれているか、悪意のある Web サイトにホストされている可能性があります。影響を受ける Outlook のバージョンで不正な形式の E メールメッセージを表示またはプレビュー表示することによって、この脆弱性が悪用されることはありません。特別に細工された Word ファイルを攻撃者が作成することにより、この脆弱性が悪用されてリモートでコードが実行される可能性があります。

Cisco Security Agent によるエクスプロイトの阻止

Cisco Security Agent のデフォルト ポリシーには複数のルールが含まれており、エクスプロイトによる被害を回避できます。こうした保護を実行するために、Cisco Security Agent のバイナリを更新したり、デフォルト設定を変更する必要はありません。

デフォルトのセキュリティ ポリシーを適用した Cisco Security Agent では、以下のアクションがブロックされることが確認されています。

- 信頼できないリモート アプリケーションによるシステム ファイルの修正
- バッファ オーバーフローによる、バッファからのシステム機能の実行

図 1 に、このテスト結果を示します。

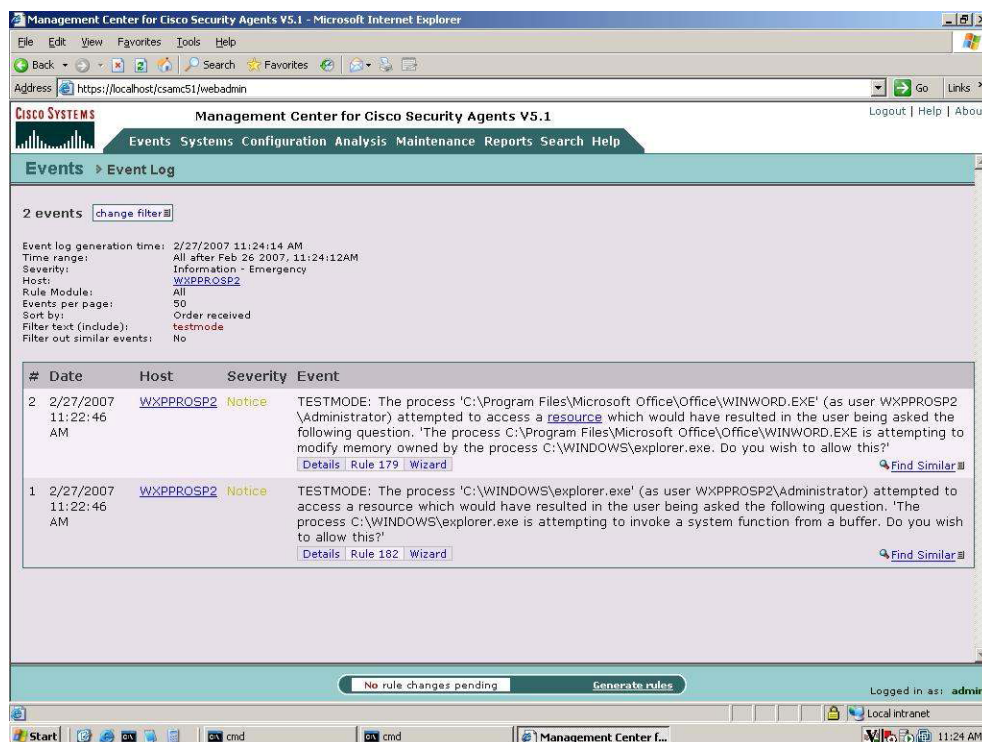
注: シスコでは、エージェントをテスト モードにしてエクスプロイトをテストしました。テスト モードでは、悪意のある振る舞いに対し警告を発行します（ブロックはしません）。このテストにより、Cisco Security Agent のデフォルト ポリシーを設定した状態で、エクスプロイトを阻止するすべての方法が監視されることを確認しました。エージェントをプロテクト モード（一般的な動作設定）にすると、最初のルールによってエクスプロイトが阻止されます。エクスプロイトは悪意ある動作を実行する前に処理され、以降のイベントは発生しません。

テストは、Cisco Security Agent のデフォルト ポリシーに対して実施しました。Cisco Security Agent を有効に機能させるために、バイナリまたはポリシーの更新は必要ありませんでした。つまり、文字通りの「Day Zero」保護のテストだと言えます。シスコでは、過去のエクスプロイトおよびワームの場合と同様に、バイナリまたはポリシーの更新を実行することなく、Cisco Security Agent のデフォルト設定によってエクスプロイトを阻止できることを確認しました。次のリストは、Cisco Security Agent のデフォルトのセキュリティ ポリシー設定によって阻止された、過去のワームおよびエクスプロイトの一部です。

エクスプロイト	ワーム	エクスプロイト	ワーム
Bagle	E メール ワーム	SQL Snake	ネットワーク ワーム
Blaster	ネットワーク ワーム	JPEG/GDI+	マルウェア ダウンローダ
Bugbear	E メール ワーム	MyDoom	E メール ワーム
Code Red	ネットワーク ワーム	Nimda	ネットワーク ワーム
Debplot	ネットワーク ワーム	Pentagone/Gonner	E メール ワーム
Fizzer	E メール ワーム	Sasser	ネットワーク ワーム
Gator/Gain	スパイウェア	Sircam	E メール ワーム
Hotbar	スパイウェア	Sobig	E メール ワーム
SQL Slammer	ネットワーク ワーム	Zotob	ネットワーク ワーム

今回のエクスプロイトは、組織のコンピューティング環境およびネットワーク環境に深刻な打撃を与え、発生と変化を続ける攻撃の 1 つにすぎません。このような新しい攻撃を阻止するために重要なことは、デフォルト設定に変更を加えることなく攻撃を阻止できる能力、およびデフォルト ポリシー内のさまざまなルールによる多層型防御の 2 点を実現することです。

図 1 Cisco Security Agent のデフォルト設定による MS07-014 エクスプロイトの阻止 (Cisco Security Agent 5.1 でテストを実行)



©2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0701R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日 10:00～12:00、13:00～17:00

お問い合わせ先